VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO FIN DE GRADO

GRADO EN DERECHO

Departamento de Derecho Administrativo, Financiero y Procesal

Derecho Procesal

Curso 2019/2020

Sistemas de interceptación masiva de las comunicaciones. Protección en la regulación española

Enrique José Varela Pampín

Tutor / Alicia González Monje

Junio 2020

TRABAJO FIN DE GRADO

GRADO EN DERECHO

Departamento de Derecho Administrativo, Financiero y Procesal

Derecho Procesal

Sistemas de interceptación masiva de las comunicaciones. Protección en la regulación española

Mass surveillance systems. Protection in spanish regulation

Nombre del/la estudiante: Enrique José Varela Pampín
e-mail del/a estudiante: enriquejpampin@gmail.com

Tutor/a: Alicia González Monje

RESUMEN

Uno de los hechos clave a nivel político de la última década fueron las revelaciones hechas por Edward Snowden acerca de los programas que los Estados Unidos junto con otros Estados venían llevando a cabo con el objetivo de interceptar comunicaciones relevantes realizadas a través de cualquier medio, ya fuera telefónico o a través de Internet. Aunque de la existencia de algunos se tiene constancia desde principios del siglo XXI (ECHELON), otros han sido desarrollados y descubiertos en esta última década. Su objetivo aparente es la lucha contra el terrorismo, y de hecho, desde el ataque de Al Qaeda a las Torres Gemelas en septiembre de 2001, han proliferado enormemente. Sin embargo, esconden todo un entramado de espionaje político que ha alcanzado incluso a Presidentes y Primeros Ministros de importantes países, y en ocasiones ha sido empleado para que empresas nacionales de los involucrados logren ventajas económicas en el mercado.

Frente a esto, en Europa se ha reforzado la protección de los ciudadanos ante estas amenazas mediante la obligatoria adhesión de los Estados miembros de la Unión Europea al Convenio Europeo para la Protección de los Derechos Humanos, con base en el cual el Tribunal Europeo de Derechos Humanos ha establecido los requisitos que deben reunir las legislaciones nacionales para respetar los derechos fundamentales de sus ciudadanos.

PALABRAS CLAVE: ECHELON, interceptación masiva, intimidad, Tribunal Europeo de Derechos Humanos, comunicaciones.

ABSTRACT

One of the main politic facts in the last decade was the revelations made by Edward Snowden about the programs that the United States with other States have been made with the objective of the interception of important communications made by any way of communication: by phone or by the Internet. Even if the existence of some of them was known since the beginning of the 21st century (ECHELON), some of them has been developed and discovered in the last century. Their apparent objective is the fight against terrorism, and, in fact, since the Al Qaeda attack to the Twin Towers in September of 2001, it has proliferated hugely. However, they hide a complicated politic espionage network that has reach Presidents and First Ministers of many important countries, and sometimes it has been used for the benefit in the market of national business.

In front of that threats, Europe has improve in the protection of the citizens, by the necessary adhesion of the European Union members to the European Convention on Human Rights, which is the main base for the European Court of Human Rights to create the requirements that national legislations must respect in order to protect the fundamental human rights of their citizens.

KEYWORDS: ECHELON, mass surveillance, Human Rights European Court, privacy, communications.

ÍNDICE

1. Introducción

1.1 Objeto

El presente trabajo se dedica al estudio de los sistemas de interceptación masiva de las comunicaciones que han surgido durante el siglo XX y principios del XXI, desarrollados por las agencias de seguridad nacionales, principalmente de Estados Unidos y Reino Unido, que trabajan en estrecha colaboración. La falta de consenso internacional en cuanto a su regulación y, sobre todo, en cuanto a la prevención de injerencias por parte de autoridades extranjeras, pone de relieve la vulnerabilidad de los derechos fundamentales garantizados en los textos internacionales de derechos humanos, dado que en esta materia no se ha establecido ningún Tribunal que tenga competencia sobre este tipo de hechos.

A ello se suma que, aunque los Estados participen en convenios internacionales que se refieran a la interceptación de las comunicaciones, o incluyan en sus normas supremas el secreto de las mismas como un derecho fundamental de los ciudadanos, la realidad es que en la práctica se diseñan normas que permiten a las agencias de seguridad e inteligencia llevar a cabo intromisiones en las mismas, fundamentalmente a través de la invocación de la lucha contra delitos socialmente muy reprochables y de gran preocupación por su magnitud y alcance, como son el tráfico de drogas o el terrorismo, principalmente este último.

En las últimas décadas, la cruzada iniciada por los presidentes de Estados Unidos contra diversos grupos terroristas de origen islámico ha tenido como consecuencia la promulgación de determinadas normas que, amparándose en el deber del Estado de proteger la seguridad y el bienestar colectivo, restringen en la práctica derechos fundamentales de sus ciudadanos, agravándose las consecuencias por el hecho de que en la gran mayoría de los casos las personas afectadas por este tipo de medidas no llegan a conocer nunca que han sido víctimas de una injerencia de este calibre en sus derechos y libertades.

1.2 Justificación y metodología

A pesar de la atención que han recibido estas cuestiones en los últimos años, a raíz de las revelaciones de Edward Snowden, ex integrante de la Agencia de Seguridad Nacional de Estados Unidos, y Julian Assange, fundador de WikiLeaks, he considerado necesaria

la recopilación de la información más relevante de la que disponemos hasta el momento en cuanto al origen de la interceptación masiva de las comunicaciones, los actores involucrados y los mecanismos a través de los cuales se produce, así como los medios de defensa con que cuentan los ciudadanos de Europa para exigir a sus respectivos legisladores la mayor protección de su derecho fundamental al secreto de las comunicaciones.

Se trato por tanto de una revisión sistemática de publicaciones doctrinales de diversas revistas del mundo jurídico, a las que se añaden informes elaborados por organismos estatales como el Congreso de Estados Unidos, y supranacionales como la Unión Europea, que a través de sus instituciones ha desarrollado una amplia labor de investigación. Por último, se han revisado diversas sentencias del Tribunal Europeo de Derechos Humanos en relación con el secreto de las comunicaciones, que a través de su jurisprudencia a elaborado un conjunto de requisitos que deben reunir las legislaciones de los Estados que se encuentran bajo su jurisdicción, para que sean consideradas acordes a la norma internacional de referencia, el Convenio Europeo para la Protección de los Derechos Humanos.

2. Antecedentes

2.1. La importancia de las comunicaciones

A efectos del presente trabajo puede definirse la comunicación como la transmisión por parte de una persona (el emisor) a otra (el receptor) de determinada información (mensaje), mediante la utilización de un código que ambos pueden compartir, y por una determinada vía. Esta comunicación puede ser tanto verbal como no verbal; la comunicación verbal puede ser tanto oral como escrita, mientras que la comunicación no verbal hace referencia a otras cuestiones relacionadas con la manera en que el emisor se comporta cuando transmite su mensaje: la postura corporal que adopta, el tono de su voz, los gestos con los que acompaña el mensaje, adónde dirige su mirada, etc.[1]

En cuanto a la comunicación verbal, el primer medio de transmitir información a personas que se encuentran en un lugar distinto del emisor fue el correo postal. Aunque este método se sigue utilizando en la actualidad, ha perdido la importancia que tuviera antes de la invención de los canales de comunicación instantánea de los que disponemos

[1] FAJARDO URIBE, L.A. "A propósito de la comunicación verbal", *Forma y función*, 2009, volumen 22, nº2, pp. 121 a 142.

hoy en día, pero da cuenta de la importancia que tuvo cuando era el único método fiable para transmitir información salvando grandes distancias sin que el mensaje se tergiversara, como ocurría con la transmisión oral. Sin embargo, por su propia naturaleza, este medio estaba muy expuesto a peligros como la pérdida del mensaje o su apertura, dado que hasta la invención de las máquinas de vapor el trayecto tenía que realizarse a pie.

En siglos más recientes comenzaron a surgir algunos aparatos que permitieron salvar este inconveniente, pues la información se transmitiría por cables instalados a lo largo de un vasto territorio. El telégrafo eléctrico fue el primero, y le seguirían otros ya más modernos como la radio o el teléfono. Su importancia sería capital en la transformación económica, social y política de los últimos siglos, favoreciendo además la globalización de la información, pues de esta manera un determinado hecho podría ser conocido en distintas partes del mundo al poco tiempo de suceder[2].

La parte negativa de estos avances es que su intervención a gran escala es mucho más sencilla y eficaz que la del correo postal. En poco tiempo se puede reunir una cantidad ingente de información personal acerca de los involucrados y, sobre todo, sin que éstos tengan noticia de tal invasión. La protección a todas las personas que puedan sufrir hechos de este tipo se hizo, pues, obligatoria.

Las comunicaciones jugaron un papel fundamental en el pasado reciente, en uno de los acontecimientos más escalofriantes de la historia moderna: la Segunda Guerra Mundial. Durante los años que duró esta contienda, los involucrados eran perfectamente conscientes de que el bando contrario disponía de los medios suficientes para interceptar sus comunicaciones. Por ello, los alemanes inventaron el que es considerado el primer ordenador moderno: la máquina Enigma.

La principal función de Enigma era el cifrado de los mensajes que los mandos militares alemanes transmitían a las diferentes secciones del ejército, con información y órdenes sobre cómo actuar. Averiguar su funcionamiento se tornó de gran importancia para acortar la duración de la guerra y asegurar la victoria de los aliados. Éste era increíblemente complejo, y se basaba, básicamente, en un algoritmo[3] de sustitución de

[2] JOSKOWICZ, J. "Breve historia de las telecomunicaciones". *Instituto de Ingenieria Eléctrica de la republica de Uruguay,* 2013.

[3] Cifrado de Vigenère: data de 1553, y consiste en la sustitución de las letras de un alfabeto por otras siguiendo una tabla colocada en el eje x, y; en la que en ambos ejes se van colocando las letras. La combinación se realiza comenzando desde la letra de cada eje y avanzando tanto vertical como horizontalmente siguiendo el orden normal en el alfabeto. Para cifrar el mensaje se

letras. El criptoanalista británico Alan Turing tuvo un papel esencial en aquel momento, cuando logró contrarrestar la técnica alemana, lo cual tuvo un gran impacto en la prevención de destrucción de bases militares y buques de guerra por parte del ejército del aire alemán y sus barcos.

Estos hechos tendrían gran trascendencia en el desarrollo de los acontecimientos inmediatamente posteriores a la guerra, y cuyos efectos se extenderían a lo largo de la segunda mitad del siglo XX hasta alcanzar el momento actual, en lo que a intervención secreta de las comunicaciones, tanto individual como masivamente se refiere.

2.2. El bien jurídico protegido: intimidad vs. privacidad

El concepto de bien jurídico protegido surge como reacción al más estricto positivismo jurídico, pensamiento doctrinal que aboga por una interpretación muy limitada de las reglas que pueden servir de fuente a los órganos jurisdiccionales para tomar decisiones en los asuntos que deban resolver. A pesar de que en los últimos siglos experimentó una evolución constante debido a las críticas de sus múltiples detractores, de forma muy resumida se podría decir que el positivismo plantea que los jueces y tribunales deben utilizar preferentemente la ley escrita como guía de actuación en sus resoluciones, y se oponen fervientemente a la utilización de principios abstractos[4].

Esta línea de pensamiento nació ligada a las Revoluciones liberales del siglo XVIII, de las que toma sus notas características. La base de sus planteamientos se encuentra en el principio democrático y la separación de poderes: las leyes deben ser elaboradas por los representantes del pueblo, el legislador, y este hecho es al mismo tiempo lo que otorga legitimidad a la Ley. Dado que las leyes emanan de la voluntad popular, los jueces deben ceñirse a lo que establecen, pues ellos no disponen de la misma legitimidad por no ser los representantes de la voluntad popular. En caso de que decidieran contradecir la ley o

necesita conocer la posición de cada letra del mensaje a cifrar en el alfabeto, la de las letras que compongan la clave y el número total de letras. Así, mediante la fórmula matemática C(Xi) = (Mi + Ci) \mod L , donde M es la posición de la letra del mensaje en el alfabeto, C la de la letra clave y L la longitud del mismo, se obtiene otro grupo de letras. [ESTEVE ROMERO, Abel. *Arqueología informática: Implementación de sistemas clásicos de cifrado en Scratch*. MOLERO PRIETO, Xabier (dir.). Tesis Doctoral. Universitat Politècnica de València. Departamento de Informática de Sistemas y Computadores, 2019.]

[4] Consulta sobre positivismo jurídico. En WOLTERS KLUWE: *soluciones integrales de información, software, conocimiento y formación*. [en línea]. Disponible en: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAUNTY1NjtbLUouLM_DxbIwMDC0MDI3OQQGZapUt-ckhlQaptWmJOcSoAaUZUozUAAAA=WKE [Consulta: 6-3-2020].

trataran de enmendarla, estarían contradiciendo la voluntad popular o usurpando el poder legislativo que corresponde al Parlamento.

En oposición a esta forma de entender el Derecho, surgieron otras que abogaban por la imposibilidad de que el legislador pudiera prever de forma general todos los casos que la ley debe amparar para proteger a los ciudadanos. De esta manera se extendió la utilización de principios que serían la referencia fundamental en caso de que la ley no fuese lo suficientemente clara respecto de cómo resolver una controversia, siendo los más importantes el principio de legalidad[5], la no discriminación y el principio de igualdad. Así, surgieron una serie de elementos abstractos que serán los que la ley concreta trate de proteger: los bienes jurídicos[6]. Se pueden definir como aspectos de la realidad social que son importantes para la comunidad, interesada en su conservación y protección. Respecto del objeto del presente trabajo, la intervención de comunicaciones, el bien jurídico protegido será la intimidad o la privacidad, en función del contexto en el que nos situemos.

El derecho a la intimidad se encuentra entre los derechos fundamentales ligados a la personalidad, reconocido desde el siglo XIX, incluso antes que los derechos sociales. Su delimitación es compleja debido a que su contenido es cambiante, además de que la utilización de sinónimos para hacer referencia a la intimidad es bastante frecuente; destacan algunos como la privacidad, el secreto o la confidencialidad[7]. La confusión es particularmente elevada entre la intimidad y la privacidad, pues en la doctrina hay un debate importante en torno a si es correcto utilizar ambos términos como sinónimos.

En este sentido, DÍAZ ROJO es una de las principales figuras que han contribuido a delimitar ambos conceptos. Así, señala que "*el hecho de que una unidad léxica esté registrada en un diccionario sea este diccionario descriptivo o normativo, es un indicio de que es correcta, y, por tanto, de que puede emplearse sin incurrir en un error*"[8].

[5] El principio de legalidad establece que ninguna conducta puede ser castigada si no ha sido prevista con anterioridad en una ley.

[6] DÍEZ RIPOLLÉS, J.L. "El bien jurídico protegido en el Derecho penal garantista". *Jueces para la democracia*, 1997, nº 30, pp. 10 a 19.

[7] GONZÁLEZ PORRAS, A. J. *Privacidad en internet: los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva*. PÉREZ PEDRERO, E.B. (dir.). Tesis doctoral, Universidad de Castilla-La Mancha, Departamento de Derecho Constitucional. 2016.

[8] DÍAZ ROJO, J.A. "Privacidad: ¿neologismo o barbarismo?" *Espéculo. Revista de Estudios*, 2002.

El Diccionario de la Lengua Española (RAE) define la privacidad como el "*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*"[9]. Al mismo tiempo, define lo privado como aquello que "*se ejecuta a la vista de pocos, familiar y domésticamente, sin formalidad ni ceremonia alguna*"[10]. El término "privado" proviene del latín *privatus*, muy relacionado con la propiedad privada entendida como lo contrario a lo público. Hace referencia al derecho de los individuos a aislarse de los demás, a tener un espacio propio en el que no ser molestado. Este concepto fue desarrollado en el ámbito del derecho anglosajón. Debido a la connotación de propiedad que tiene este término, no puede entenderse como sinónimo de intimidad, cuyo significado es diferente.

El término "intimidad", por el contrario, no nació en el derecho anglosajón, y por ello muchos estiman que su uso es más correcto que el de privacidad[11], que es una simple traducción del inglés *privacy*. La intimidad hace referencia a lo más interior o interno de una persona, su zona espiritual íntima y reservada[12]. Es aquello que se pretende esconder de los demás. Por tanto, que determinada información sea privada no tiene por qué significar que su contenido es íntimo, sino que se posee con exclusividad y debe mantenerse en secreto. Si, además de privada, es íntima, significa que dicha información se refiere a elementos profundos de la personalidad.

En síntesis, el derecho a la privacidad es propio del Derecho anglosajón, mientras que en Derecho continental lo correcto es hablar del derecho a la intimidad. La protección de cada uno de ellos también es diferente: en España, el derecho a la intimidad está previsto en el artículo 18.1 de la Constitución de 1978: "*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen"*[13]. El hecho de que se exponga junto a otros dos derechos considerados personalísimos (honor y propia imagen), que son aquellos que tienen todas las personas por el hecho de nacer, ha llevado a la doctrina a señalar que el derecho a la intimidad es también un derecho personalísimo ligado a la dignidad de la persona[14]. En cambio, el derecho a la privacidad anglosajón se encuentra

[9] REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.3 en línea]. https://dle.rae.es/privacidad?m=form [1 de marzo de 2020].

[10] REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.3 en línea]. https://dle.rae.es/privado [1 de marzo de 2020].

[11] El País, *Libro de estilo: nueva versión actualizada*, 22ª ed., Madrid, 2014.

[12] REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.3 en línea]. https://dle.rae.es/intimidad?m=form [Consulta: 1 de marzo de 2020]

[13] Art. 18.1 de la Constitución Española de 1978. España. Constitución Española. *BOE* núm. 311, 29 de diciembre de 1978, pp. 29313 a 29424.

[14] GONZÁLEZ PORRAS, A. J. *Privacidad en internet…*, op., cit., p. 5

recogido, por ejemplo, en la Cuarta Enmienda de la Constitución de Estados Unidos[15], de la siguiente manera: "*El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas"*. Parece evidente que la Constitución americana es mucho más generalista en su protección, y va más allá de lo que se entiende por intimidad.

2.2.1.1. La interpretación jurisprudencial de la privacidad en Estados Unidos

La conexión con el objeto del presente trabajo se produce en el siglo XX, cuando el Tribunal Supremo de Estados Unidos optó por una interpretación literal de las garantías frente a registros arbitrarios, de manera que exigía la intrusión física en los domicilios, documentos y efectos personales para que se considerara infringido el precepto constitucional. Las escuchas mediante aparatos electrónicos no supondrían una violación de la Cuarta Enmienda porque, en opinión del Tribunal, "quienes instalan en su domicilio un instrumento telefónico con cables que lo conectan al exterior se proponen proyectar su voz hacia quienes están fuera", por lo que tal cableado y los mensajes que conduce no están protegidos[16][17]. Sin embargo, BRANDEIS se apartó de la opinión mayoritaria y defendió una interpretación dinámica de la Constitución que permitiera adaptar las garantías constitucionales individuales frente a los abusos del poder. En particular, manifestó una gran preocupación hacia los avances tecnológicos, en comparación con los cuales la interpretación dada a la legislación se quedaba obsoleta. En su opinión, toda intromisión injustificada del Gobierno en la esfera privada de la persona supone una violación de la Cuarta Enmienda[18].

En la década de los 60 se inició una jurisprudencia mucho más favorable. En el caso *Mapp v. Ohio*[19] el Tribunal declaró que la Cuarta Enmienda genera un derecho a la

[15] Cuarta Enmienda de la Constitución de los Estados Unidos de América de 1787. Disponible en: https://www.constitutionfacts.com/content/constitution/files/USConstitution_Spanish.pdf

[16] Olmstead v. United States, 277 U.S. 438 (1928)

[17] NIEVES SALDAÑA, M. "El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego". *Teoría y Realidad Constitucional*, 2011, nº28, pp. 279 a 312.

[18] Idem.

[19] Mapp v. Ohio, 367 U.S. 643 (1961).

privacidad igual de importante que cualquier otro derecho especialmente reservado al pueblo, y por tanto exigible a los Estados. Esta nueva interpretación se corroboró en los casos posteriores, fundamentalmente *Berger v.s New York*[20] y *Katz v. United States*[21]. En este último, el Juez Harlan presentó el término "expectativa razonable de privacidad", por la que "*sólo existe una zona de privacidad garantizada por la Cuarta enmienda si la persona ha actuado conforme a una real expectativa de privacidad y si tal expectativa la sociedad está preparada para reconocerla como razonable*"[22].

Siguiendo esta lógica, el derecho a la privacidad se fue extendiendo a otros ámbitos personales como el matrimonio, la crianza de los hijos, la procreación, el aborto, el uso de anticonceptivos, la orientación sexual, etc.

En la actualidad, este derecho ha adquirido tintes diferentes debido a la necesidad de adaptarse a los cambios tecnológicos del último cuarto del siglo XX en adelante, que han facilitado enormemente la interceptación de las comunicaciones personales de millones de personas, proceso que comenzó tras la Segunda Guerra Mundial amparado por una serie de leyes que, tanto en Estados Unidos (principalmente) como en Europa y el resto del mundo, han permitido vulnerar tanto el derecho a la privacidad como el derecho a la intimidad de forma sistemática, amparándose en la necesidad de protección frente a las amenazas crecientes del terrorismo y de las potencias enemigas.

2.2.1.2. El derecho a la intimidad en Europa

Al contrario que en Estados Unidos, en Europa no existe una amplia jurisprudencia cambiante que haya ido perfilando y otorgando contenido al derecho a la intimidad, sino que en su lugar proliferaron ensayos doctrinales y filosóficos por parte de autores como Jeremy Bentham, Thomas Hobbes, John Locke o John Stuart Mill[23].

Las primeras Constituciones que reconocieron expresamente el derecho a la intimidad fueron la portuguesa de 1976[24] (artículo 33, *Derecho a la identidad, a la buena fama y a*

[20] Berger v. New York 388 U.S. 41 (1967): inconstitucionalidad de una ley de Nueva York que autorizaba la grabación secreta de comunicaciones por agentes encubiertos por períodos de hasta sesenta días, afirmando que las conversaciones estaban protegidas por la Cuarta Enmienda y que el uso de artefactos electrónicos para incautarlas no determina que fuesen registros constitucionalmente admisibles. En NIEVES SALDAÑA, M. "El derecho a…, op., cit., p.7

[21] Katz v. United States 389 U.S. 347, 351 (1967).

[22] NIEVES SALDAÑA, M. "El derecho a…, op., cit., p. 7

[23] ALFONSO, L.P. "El derecho fundamental a la intimidad". *Ius et Praxis*, 1993, pp. 39 a 56.

[24] Art. 33 Constitución portuguesa de 1976: "1. Se reconoce a todos el derecho a la identidad personal, al buen nombre y reputación y a la reserva de su intimidad en la vida privada y familiar. 2. La ley establecerá garantías efectivas contra la utilización abusiva, o contraria a la dignidad

la intimidad) y la española de 1978[25] (artículo 18), un poco más ampliamente que la primera.

Tal y como dice GONZÁLEZ PORRAS[26], dada la influencia filosófica y doctrinal previa, el derecho a la intimidad se configura como una garantía de la libertad personal, pues "*si la información personal o familiar es distorsionada, se divulga sin responsabilidad o se produce una intromisión no consentida, ello ocasiona un recorte o captura de la libertad, ya que tales actos no permiten que las personas adopten las decisiones de su existencia en forma libre y autónoma, sin estar afectado por la vulneración de su intimidad*."

2.3. Sistemas de interceptación de comunicaciones en los siglos XX-XXI

Tras los hechos acontecidos en la Segunda Guerra Mundial, donde la interceptación de las comunicaciones del ejército alemán fue un elemento fundamental para poner fin al conflicto bélico, algunos de los Estados beligerantes se reunieron para establecer un plan de acción común en las décadas posteriores. De esta forma se originó el denominado Convenio UKUSA, por las siglas de sus promotores (*United Kingdom* y *United States of America*), además de Australia, Canadá y Nueva Zelanda, dando inicio a una red de vigilancia que se mantendría en secreto durante décadas, y cuya infraestructura permanece vigente hoy en día.

Los Estados firmantes establecieron las actividades de interceptación, recolección, adquisición, análisis y descifrado en su zona geográfica, para posteriormente compartir con el resto la información recabada. La Agencia Nacional de Seguridad (NSA) de Estados Unidos fue creada bajo este contexto en 1952 por el presidente Harry Truman. Y se conoce que, en 1960, siendo presidente J. Edgar Hoover, el FBI recopiló una inmensa cantidad de información personal de diversos personajes políticos, entre ellos Martin Luther King Jr.

---

humana, de informaciones relativas a las personas y a las familias." [Disponible en: http://confinder.richmond.edu/admin/docs/portugalsp.pdf]

[25] Art. 18 CE: "1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

[26] GONZÁLEZ PORRAS, A.J. *Privacidad en internet…*, op., cit., p. 5

2.3.1.1. El sistema ECHELON

Echelon es el nombre clave dado para una red de vigilancia de comunicaciones privadas y económicas, que nació en el marco del Acuerdo UKUSA en 1971. En esta red participaban fundamentalmente cinco países: Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda[27]. Así lo expuso el Parlamento Europeo el 11 de julio de 2001 en un informe completo sobre el funcionamiento de este sistema, con el propósito añadido de crear un Comité temporal de investigación y debate[28].

Esta red abarcaba todos los sistemas de comunicación e información, incluidos correos electrónicos, llamadas fijas y móviles, mensajería instantánea, faxes, blogs, internet, etc., a través de un complejo entramado de satélites interconectados entre si. El seguimiento se produce a partir de la detección de una comunicación concreta que contiene palabras clave anteriormente predefinidas, o combinaciones de palabras, a partir de lo cual el sistema graba, etiqueta y envía (con número clave identificativo) a distintos centros de análisis, donde se transcriben, descifran y guardan. Y dado que el Acuerdo UKUSA tenía como premisa fundamental la cooperación mutua entre los participantes, los resultados se enviaban al resto de agencias de inteligencia[29].

En la propuesta de resolución del Parlamento Europeo[30], Considerando B, se expresa que "*no cabe ninguna duda*" de que la finalidad del sistema es la interceptación, como mínimo, de comunicaciones privadas y económicas. Sin embargo, precisa que la capacidad del sistema era mucho menor del que se había supuesto en un principio y de lo que se había expuesto en los medios de comunicación. Además, el órgano no era ajeno al hecho de que la red de interceptación se utilizaba con otros fines además de garantizar la seguridad nacional, concretamente el espionaje industrial. Según fuentes autorizadas que confirmaron el informe Brown del Congreso estadounidense, esta vigilancia en materia de inteligencia podría permitir a la industria estadounidense ganar hasta 7.000 millones de dólares en los contratos. A pesar de ello, en aquel momento dicha conducta no violaba el Derecho de la, entonces, Comunidad Europea, pues las Directivas de Protección de

[27] Por este motivo se conocería al grupo como el *Five Eyes*, que por la situación de sus territorios y los de ultramar de cada uno de ellos les permitía la interceptación de las comunicaciones privadas de la práctica totalidad del globo.

[28] PARLAMENTO EUROPEO. *Informe sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON)* (2001/2098 (INI)), 2001, pp. 64 a 68.

[29] MALDONADO, C.E. "La red Echelon: el control de internet y de todas las comunicaciones". *Le Monde diplomatique*, 2013, p. 30-31.

[30] PARLAMENTO EUROPEO. Informe sobre…, op. cit., p. 9

Datos vigentes (95/46 y 97/66) no se aplicaban al tratamiento de datos que tuviera por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal.

En cambio, sí se consideraría producida una violación del Derecho comunitario en el caso de que un Estado miembro recurriera a un sistema de interceptación que incluyera el espionaje en materia de competencia. El Parlamento, sin embargo, en ese informe de 2001 determinó que en base a la situación jurídica vigente, ECHELON no violaba el Derecho de la Comunidad, salvo que se demostrara efectivamente su utilización para el espionaje en materia de competencia. Distinto será el caso con otro tipo de normas internacionales, fundamentalmente el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos.

2.3.1.2. La Ley de Vigilancia de Inteligencia Extranjera (FISA)

En 1972 estalló el llamado *Watergate*, un caso de espionaje político en Estados Unidos, tras cuya investigación se reveló que el por aquel entonces presidente Richard Nixon estaba involucrado. Nixon dimitiría en 1964 tras conocerse que disponía de un sistema de grabación de cintas magnéticas en sus oficinas y que se habían grabado un gran número de conversaciones. Debido a estos hechos, el Senado de Estados Unidos creó un Comité presidido por Frank Church; tras sus investigaciones, declaró que Estados Unidos disponía de un amplio sistema que permitía captar todos los mensajes enviados a través del aire.

La Ley de Vigilancia de Inteligencia Extranjera (FISA) se promulgó en 1978 a raíz del informe presentado por el senador Church. Básicamente, permite llevar a cabo la vigilancia electrónica con el fin de obtener información de inteligencia extranjera sin que fuera necesario requerir una orden judicial de arresto previa. Para ello se estableció un Tribunal que sería el encargado de autorizar la vigilancia, lo cual solamente sería posible si existía un motivo razonable para creer que el objetivo formaba parte de la inteligencia extranjera y las instalaciones que se habrían de vigilar serían utilizadas por una potencia extranjera de la cual se pudiera prever un relativo esfuerzo por atacar, sabotear o realizar actos de terrorismo internacional[31].

[31] SANTOS, F.R. "El Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos de América y la propuesta de lege ferenda en el derecho comunitario". *Diario La Ley*, 2017, p. 2.

Esta ley se enmendaría nuevamente en el año 2008 bajo el mandato de George W. Bush para permitir programas de vigilancia masiva a extranjeros, incluso fuera del territorio estadounidense[32].

2.3.1.3. La lucha contra el terrorismo global

El 11 de septiembre de 2001, apenas unos días después de que el Parlamento Europeo emitiera su informe y propuesta de solución respecto del sistema ECHELON, se produjo el atentado contra las Torres Gemelas, cuando dos aviones impactaron contra ambos edificios, otro contra el Pentágono y un cuarto en un parque a las afueras de Pennsylvania. El ataque fue perpetrado por miembros del grupo terrorista Al-Qaeda, y desencadenaría múltiples reacciones armadas por parte de Estados Unidos, así como una "guerra" que se libraría desde el plano jurídico[33].

La Ley Patriota (USA-Patriot Act) se aprobó ese mismo año 2001, y su principal efecto fue la ampliación de las capacidades de vigilancia del gobierno. También modificó otras leyes, entre ellas la de Vigilancia de Inteligencia Extranjera y algunas relacionadas con las comunicaciones y la privacidad (por ejemplo, la Ley Omnibus de Control de la Delincuencia y Seguridad de las Calles de 1968).

Desde entonces, la interceptación de comunicaciones por la Agencia de Seguridad Nacional de Estados Unidos ha sido constante. Lo es hoy en día y también tuvo una gran trascendencia en los últimos años debido al surgimiento de un nuevo grupo terrorista que por momentos amenazó con desestabilizar la paz y la seguridad de occidente: DAESH.Además de su presencia en Siria, destacan los atentados de París[34], Niza[35],

[32] MARTÍN LÓPEZ, S. *Programas de vigilancia de Internet*. PÉREZ SOLÀ, C. (dir.). Trabajo de FIN DE MASTER, Universitat Oberta de Catalunya, Máster Interuniversitario en seguridad de las tecnologías de la información y de las comunicaciones (MISTIC), 2014.

[33] TELEMADRID. 2019. Se cumplen 18 años del atentado terrorista del 11-S. [en línea]. 11 de septiembre de 2019. Disponible en: http://www.telemadrid.es/programas/telenoticias-1/anos-atentado-terrorista-11-S-2-2157704242--20190911043523.html [consulta: 8 de marzo de 2020]

[34] LA RAZÓN. 2019. La barbarie yihadista relatada desde dentro del Charlie Hebdo. [en línea] 29 de agosto. Disponible en: https://www.larazon.es/cultura/la-barbarie-yihadista-relatada-desde-dentro-del-charlie-hebdo-LD24729165/ [consulta: 8 de marzo de 2020]

[35] YÁRMOS, C. 2016. El ISIS se responsabiliza de la matanza de Niza. *El País*. [en línea] 16 de julio. Disponible en: https://elpais.com/internacional/2016/07/16/actualidad/1468654029_015759.html [consulta: 8 de marzo de 2020]

Berlín[36] o Londres[37], que comparten una serie de características que hacen a este terrorismo completamente diferente de lo experimentado hasta entonces[38]:

- En primer lugar, destaca el amplio abanico de opciones que presenta, desde grupos conectados a través de la red hasta individuos solitarios; ataques directos de DAESH o inspirados por éste; uso de explosivos, rifles, armas blancas o vehículos; y sobre todo ataques preparados minuciosamente frente a otros que parecen espontáneos.
- La actuación de individuos en solitario dificulta enormemente la tarea de investigación, pues además raramente seleccionan objetivos con carga simbólica, sino que muestran una preferencia por objetivos vulnerables y fácilmente alcanzables.
- Además de la pérdida de vidas humanas, buscan también que los ataques tengan cierto impacto económico.
- Los actores suelen ser personas radicalizadas sin necesidad de que tengan una convicción profunda.
- En Siria, las posibilidades de crear centros de entrenamiento fueron muy alto durante cierto tiempo.
- Debido a que tenían una notable presencia en redes sociales, los individuos y grupos extremistas hicieron un uso extensivo de la encriptación para que sus comunicaciones no fueran detectadas por las autoridades y agencias de inteligencia.

El ataque terrorista del 11 de septiembre de 2001 fue perpetrado por un grupo con una vinculación muy fuerte con los que posteriormente fundarían el DAESH, y la respuesta inmediata, como hemos visto, fue ampliar las competencias del gobierno y de la Agencia de Seguridad Nacional para intervenir las comunicaciones de millones de personas, con la justificación de luchar contra el terrorismo. A partir de entonces surgieron múltiples formas de espionaje e interceptación de comunicaciones, de los cuales se puso seriamente en duda que su objetivo único fuese la seguridad nacional.

[36] CNN. 2016. ISIS dice que motivó el ataque en Berlín. [en línea] 20 de diciembre. Disponible en: https://cnnespanol.cnn.com/2016/12/20/isis-se-atribuye-responsabilidad-del-ataque-en-berlin/ [consulta: 8 de marzo de 2020]

[37] EL ESPAÑOL, 2019. Estado Islámico reivindica el atentado del Puente de Londres: "Fue uno de nuestros combatientes". [en línea] 30 de noviembre. Disponible en: https://www.elespanol.com/mundo/20191130/islamico-reivindica-atentado-puente-londres-combatientes/448455641_0.html [consulta: 8 de marzo de 2020]

[38] EUROPOL. Changes in modus operandi of Islamic State (IS) revisited'. *The Hague*, 2016.

2.3.1.4. Programas posteriores a ECHELON: PRISM y TEMPORA

En junio de 2013, el periódico *The Guardian* publicaba en exclusiva que la Agencia Nacional de Seguridad (NSA) tenía acceso a toda la información de los clientes de la operadora de telecomunicaciones *Verizon*[39]. El origen de las filtraciones fue un exagente de la NSA llamado Edward Snowden, que con la publicación de una gran cantidad de información secreta a la que tenía acceso reveló al mundo el espionaje masivo de Estados Unidos y el resto de los países que conformaban el grupo *Five Eyes*. Lo primero que se supo fue que el Tribunal de Vigilancia de Inteligencia Extranjera (FISA) creado con la ley de 1978 había emitido una orden secreta a la empresa Verizon Business, una de las más grandes teleoperadoras del país, en la que se le exhortaba a entregar todos los registros de sus clientes, tanto en Estados Unidos como del exterior. También permitía a la NSA recoger información de organismos como el Banco Central Europeo, el Fondo Monetario Internacional o la Unión Europea[40].

En los días y meses siguientes se fueron revelando nuevas informaciones respecto de la vigilancia indiscriminada llevada a cabo durante décadas por Estados Unidos:

El 7 de junio de 2013[41] se reveló el programa PRISM. La llamada Ley de Protección de América (The Protect America Act) permitió jurídicamente en 2007 a la NSA crear este programa como versión mejorada de otras iniciativas implantadas a raíz de los atentados del 11 de septiembre de 2001. PRISM era ejecutado con la colaboración de grandes empresas como Microsoft, Facebook, Google, Apple, Yahoo, Skype, YouTube, AOL o PalTalk, tal y como informó The Washington Post[42]. Este programa permitía recoger tanto el contenido de los correos, llamadas, archivos almacenados, chats, etc.,

---

[39] GREENWALD, G. 2013. NSA collecting pone records of millions of Verizon customers daily. *The Guardian*. [en línea] 6 de junio. Disponible en: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [consulta: 8 de marzo]

[40] VANDERLINDER, I. "Los derechos humanos ante la vigilancia indiscriminada de las comunicaciones privadas". *Revista UVM*. 2016, volumen 10, nº2. Disponible en: http://revistav.uvm.edu.ve/articulos/n41bliArticulo04vol10num22016.pdf [consulta: 10-3-2020].

[41] DOULIERY, O., 2013. EE. UU. tiene acceso a datos de los servidores de Facebook, Google, Apple, Yahoo o Skype. *20 Minutos*. [en línea] 7 de junio. Disponible en: https://www.20minutos.es/noticia/1836839/0/obama-espionaje-servidores/google-facebook-skype/seguridad-nacional/ [consulta: 10 de marzo de 2020]

[42] GELMANN, B., 2013. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. [en línea]. Disponible en: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [consulta: 10 de marzo de 2020]

como el registro de llamadas, nombre los participantes, hora, duración, número de serie del aparato empleado, números de teléfono, etc.

Unos días después, Snowden declaró que los Gobiernos de Estados Unidos establecieron de forma sistemática un mecanismo de espionaje sobre sistemas de telecomunicaciones de China y Rusia, que se prolongó durante años. Al mismo tiempo se reveló también la participación del GCHQ, los servicios de inteligencia de Reino Unido, en colaboración con los estadounidenses, con el objetivo de recabar información relativa a políticos participantes de las principales cumbres mundiales (G8 y G20, así como de Naciones Unidas.

TEMPORA fue revelado también al poco tiempo. El jornal estadounidense *The Washington Post* informó de que la Agencia de Seguridad Nacional de Estados Unidos había almacenado más de un cuarto de billón de cuentas de correo electrónico (principalmente Gmail) y contactos de redes sociales como Yahoo o Facebook. A la par de estos hechos, informaron de la intervención, en colaboración con los servicios británicos, de los cables de fibra óptica submarinos que circulan y conectan ambos continentes[43].

En este programa se vieron involucradas diversas compañías de telecomunicaciones, como BT, Verizon Business, Vodafone Cable, Global Crossing, Level 3, Viatel e Interoute, y al igual que en el caso de PRISM se recogían tanto el contenido como los metadatos[44].

En los meses que siguieron continuó revelándose información acerca de la participación de la NSA en otros programas clandestinos de espionaje a miembros de gobiernos extranjeros, altos cargos de empresas transnacionales, entidades bancarias relevantes y gran cantidad de medios de comunicación de distintos Estados. Se incluye entre ellos a los gobiernos de España, Italia, Venezuela o Colombia.

Los usuarios también vieron vulnerada su intimidad en relación con su imagen, puesto que se descubrió la intervención de webcams, lógicamente sin consentimiento del usuario, por parte de los servicios británicos, que enviaron la información recolectada a la NSA.

[43] RIVERA, N., 2016. Cronología del caso Snowden, el hombre más buscado el mundo. *Hipertextual*. [en línea] 15 de marzo. Disponible en: https://hipertextual.com/2016/03/cronologia-edward-snowden [consulta: 10 de marzo de 2020]

[44] MARTÍN LÓPEZ, S.. *Programas de…*, op., cit., p. 12

A mediados de 2014, la NSA comenzó a interceptar físicamente los aparatos electrónicos que debían servir para las comunicaciones, lo cual incluye *routers*, que permiten y habilitan la conexión a la red, servidores y otros sistemas. Todo ello se realizaba antes de su exportación de EEUU para su comercialización. El mecanismo era muy simple, y bastaba con instalar sistemas de escucha e interceptación de información en los aparatos, o software que permitiera el control a distancia sin ser detectado.

Con posterioridad se han descubierto más programas con utilidades similares y alcances diferentes. Algunos de ellos son XKeyscore, Dishfire, Bullrun y Edgehill, Upstream y FASCIA:

Bullrun y Edgehill son programas dedicados a descifrar claves y sistemas de cifrados. Los documentos aportados por Snowden señalaban que la NSA utilizaba programas como estos dedicados no sólo a probar claves aleatoriamente hasta dar con la correcta sino a robarlas accediendo por "puertas traseras". Según la guía de la NSA sobre el funcionamiento de Bullrun, ambos son capaces de vulnerar sistemas de encriptado y protocolos seguros como por ejemplo HTTPS, utilizado por una gran cantidad de páginas web[45].

Dishfire es un programa para la recopilación y almacenaje de mensajes de texto, así como otra información como las llamadas perdidas e incluso los cruces de frontera, debido a que intercepta los mensajes de alerta sobre la itinerancia de datos (*roaming)*.

Xkeyscore se basaba en la combinación de 700 ordenadores repartidos por todo el mundo que extraían y clasificaban información procedente de correos electrónicos y conversaciones entre usuarios de determinadas aplicaciones y sitios web, utilizando tanto metadatos como palabras clave.[46]

Upstream era utilizado en paralelo con PRISM, y al igual que éste su principal función era intervenir las redes telefónicas y la información transmitida a Internet a través de cables y *routers*, tanto del propio Estado como de otros.

[45] QUINTANA, Y., 2014. Todos los programas de espionaje de la NSA desvelados por Snowden. *Eldiario*. [en línea]. 19 de marzo. Disponible en: https://www.eldiario.es/turing/vigilancia_y_privacidad/NSA-programas-vigilancia-desvelados-Snowden_0_240426730.html [consulta: 10 de marzo de 2020]

[46] FERRER MORINI, T., 2013. Diccionario del espionaje digital. *El País*. [en línea]. 26 de octubre. Disponible en: https://elpais.com/internacional/2013/10/26/actualidad/1382810941_379301.html [consulta: 10 de marzo de 2020]

FASCIA es un enorme almacén de información, propiedad de la NSA, que cuenta con miles de millones de datos sobre la geolocalización de teléfonos móviles, obtenidos a partir del rastreo de la ubicación de los dispositivos.

2.4. La protección internacional

Los hechos narrados anteriormente y el fuerte rechazo social hacia la intromisión de los Estados en la intimidad de los ciudadanos llevaron a que desde mediado el siglo XX se adoptasen una serie de normas internacionales, que, con el objetivo de reconocer la importancia de este ámbito personal, llaman a garantizar la protección de las comunicaciones y los datos en el territorio de los Estados.

Esto se ha hecho particularmente patente en Europa, gracias en parte a las Comunidades Europeas que se fueron gestando en paralelo a este proceso, pero no exclusivamente. También otros textos internacionales de gran relevancia en la historia reciente mencionan de alguna manera el ámbito interno de las personas, la intimidad o su privacidad.

En primer lugar, el artículo 12 de la Declaración Universal de Derechos Humanos (1948) dice lo siguiente: "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*"[47].

En segundo lugar, en 1966 se firmó el Pacto Internacional de Derechos Civiles y Políticos, del que son parte 173 Estados, pero ha sido ratificado únicamente por 74. La redacción del artículo 17 del Pacto es prácticamente idéntica a la del artículo 12 de la Declaración Universal de Derechos Humanos, pero añade las injerencias ilegales como objeto de vulneración de la vida privada, familiar, del domicilio y de la correspondencia; y los ataques ilegales a la honra y a la reputación. La diferencia es sutil, y a nivel práctico es todavía menor, dado que tanto las injerencias como los ataques prohibidos por ley se entiende que ya eran considerados como vulneradores del derecho fundamental de que se trate.

[47] ESPAÑA. Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. *BOE* núm. 243, de 10 de octubre de 1979, pp. 23564 a 23570.

Asimismo, también en Europa nos encontramos con el artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea, que declara que "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones*[48] *"*.

Cabe destacar también dos Directivas importantes del Parlamento Europeo y del Consejo, que, aunque se refieren a la protección y tratamiento de datos personales y su libre circulación, se trata de elementos ligados a la interceptación de las comunicaciones y la utilización para fines políticos, industriales o de seguridad de la información recabada. En primer lugar, la Directiva 95/46/CE[49], *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Y, en segundo lugar, la Directiva 2002/58/CE, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas*[50]. Esta última se refiere expresamente a la intimidad como el objeto de protección de esta. Ambas se articulan sobre la base del artículo 16 del Tratado de Funcionamiento de la Unión Europea, que también hace referencia a la protección de los datos de carácter personal.

En América, el primer pacto internacional del siglo XX que reconoció el derecho al respeto de la vida privada fue la Declaración Americana de los Derechos y Deberes del Hombre, firmada en la ciudad de Bogotá en 1948. En el artículo 5 incluye el derecho a la protección de la honra, la reputación y de la vida privada y familiar, que debe estar garantizado por la ley. Los artículos 9 y 10 reconocen la inviolabilidad del domicilio y la inviolabilidad y circulación de la correspondencia como derechos[51].

---

[48] ESPAÑA. Carta de los Derechos Fundamentales de la Unión Europea. *BOE* núm. 83, de 30 de marzo de 2010, pp. 389 a 403.

[49] ESPAÑA. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. *DOCE* núm. 281, de 23 de noviembre de 1995, pp. 31 a 51.

[50] UNIÓN EUROPEA. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). *DOCE* núm. 201, de 31 de julio de 2002, pp. 37 a 47.

[51]Declaración Americana de los Derechos y Deberes del Hombre. Artículo V**:** "Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar." Artículo IX**: "**Toda persona tiene el derecho a la inviolabilidad de su domicilio". Artículo X**:** "Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia."

Disponible en: https://www.derechoshumanos.net/normativa/normas/america/DADH/1948-DADH.htm#a5

Le siguió la Convención Americana sobre Derechos Humanos, también denominada Pacto de San José dado que tuvo lugar en dicha ciudad de Costa Rica del 7 al 22 de noviembre de 1969. Dentro de su Capítulo II, titulado Derechos Civiles y Políticos, reconoce el derecho de todos a no "*ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación*"[52]. Además, este reconocimiento se enmarca en la protección de la dignidad de todas las personas, de manera similar a cómo el artículo 18 de la Constitución Española de 1978 incluye el respeto a la intimidad junto al derecho al honor. Cabe destacar también que Estados Unidos firmó esta declaración en 1977, pero desde entonces no la ha ratificado ni se ha adherido a ella[53].

También en África cuentan con una Declaración de Derechos Humanos, concretamente la Carta Africana sobre Derechos Humanos y de los Pueblos, aprobada el 27 de julio de 1981 durante la XVIII Asamblea de Jefes de Estado y de Gobierno de la Organización de la Unidad Africana, celebrada en Nairobi, Kenya. Entró en vigor en 1986, y aunque no reconoce expresamente el derecho a la intimidad o a la vida privada, algunos de sus artículos ponen de manifiesto que tal es la voluntad de los firmantes. El artículo 4 dice que los seres humanos son inviolables y tienen derecho al respeto de su vida y de la integridad de su persona. El artículo 5 reconoce el derecho al respeto de la dignidad inherente al ser humano. De su lectura se desprende que es una declaración dirigida a sentar unas bases mínimas de protección para las personas africanas, más centrada en proteger derechos como la vida, la salud, la integridad y la libertad. Aún así, el reconocimiento expreso de la dignidad del ser humano abre la puerta, aunque no se mencione expresamente, al concepto de intimidad que se utiliza en Europa.

2.4.1.1. Artículo 8 Convenio Europeo para la Protección de los Derechos Humanos

Este Convenio fue firmado en Roma el 4 de noviembre de 1950, y publicado en España el 10 de octubre de 1979 , ya en periodo democrático. Ha sido firmado y ratificado por

[52] Art. 11 Protección de la Honra y de la Dignidad: "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques." [Disponible en: https://www.derechoshumanos.net/normativa/normas/america/CADH/1969-CADH.htm].

[53] Información disponible en el siguiente enlace: http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos_firmas.htm

47 Estados de la zona europea[54]. Tras las modificaciones incorporadas por el Tratado de Lisboa (2007), la Unión Europea exige la adhesión a este Convenio como requisito fundamental para poder optar al acceso, pues así se establece en el artículo 6.2 del Tratado de la Unión Europea.

Comienza aludiendo a la importancia de la Declaración Universal de Derechos Humanos proclamada apenas dos años antes por la Asamblea General de las Naciones Unidas, cuyos derechos aspira a que sean reconocidos y aplicados en todos los países miembros.

En virtud de este Convenio se establecen una serie de derechos fundamentales que los Estados Contratantes se comprometen a respetar, entre ellos el derecho al respeto a la vida privada y familiar, de manera que solamente en determinados casos graves que afecten a la propia seguridad del Estado se permiten injerencias a estos derechos por parte de las Autoridades Públicas.

Para garantizar el cumplimiento de estos derechos, los Estados decidieron someterse a la competencia del Tribunal Europeo de Derechos Humanos, con sede en Estrasburgo, Bélgica. Así se establece en el Título II del propio Convenio. Funciona de manera permanente y se compone de un número de jueces igual al de los Estados parte del Convenio, que podrán conocer de demandas individuales. Para ello se encuentran legitimadas activamente tanto las personas físicas entendidas de forma individual como colectiva (asociaciones de consumidores y usuarios, por ejemplo) y ONGs (artículo 34). La ejecución de sus sentencias definitivas es obligatoria.

Respecto del presente trabajo, el problema de la interceptación de las comunicaciones reside en que muchas veces el Estado que la realiza, el interceptado y el acto de interceptación se encuentran en diferentes lugares. Aunque no se mencionen expresamente las telecomunicaciones en el texto del Convenio, la jurisprudencia del Tribunal Europeo de Derechos Humanos ha reconocido en múltiples ocasiones que éstas se encuentran amparadas por el artículo (Sentencia Klass y otros contra Alemania[55]).

[54] Albania, Andorra, Armenia, Austria, Azerbaiyán, Bélgica, Bosnia Herzegovina, Bulgaria, Croacia, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Georgia, Alemania, Grecia, Hungría, Islandia, Italia, Letonia, Liechtenstein, Lituania, Luxemburgo, Malta, Mónaco, Montenegro, Países Bajos, Macedonia del Norte, Noruega, Polonia, Portugal, República de Moldavia, Rumanía, Rusia, San Marino, Serbia, Eslovaquia, Eslovenia, España, Suecia, Suiza, Turquía, Ucrania y Reino Unido. También la Unión Europea como institución.

[55] STEDH 6 de septiembre de 1978, as. C-5029/71, *Klass and others vs. Germany* (41)

3. El secreto de las comunicaciones en Europa: jurisprudencia del Tribunal Europeo de Derechos Humanos y art. 8 CEDH

3.1. Nociones básicas

Como ya se ha mencionado anteriormente, el secreto de las comunicaciones en Europa se protege desde su inclusión en el Convenio Europeo para la Protección de los Derechos Humanos, que tiene carácter vinculante y siendo además su ratificación obligatoria para los países que pertenezcan o pretendan adherirse a la Unión Europea. Se encuentra previsto en el artículo 8.1 de dicha norma, cuyo primer párrafo dice lo siguiente:

> "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*"[56].

A pesar de su concreción, este primer párrafo tiene una gran trascendencia y un amplio contenido. Este contenido abarca la vida privada, la vida familiar, el respeto del domicilio y el respeto de la correspondencia; sería en este último donde se enmarcaría la protección de las comunicaciones. Pero también incluye otros derechos no recogidos expresamente como la autodeterminación informativa, la protección del honor, el derecho a la educación y otros derechos personales: herencia, reconocimiento de la transexualidad, propia imagen, impugnación de la paternidad, matrimonio, divorcio, visita a los reclusos o libertad contractual[57].

- **Vida privada**: el Tribunal Europeo de Derechos Humanos entiende que dentro de este concepto se encuentra también el reconocimiento de la vida sexual, porque protege una manifestación esencialmente privada de la personalidad humana[58]. De ello se puede deducir que el Tribunal hace suya la distinción europea y anglosajona de la vida privada y la intimidad, siendo el primer concepto de una amplitud mayor. La vida privada comprende también la integridad psíquica y moral[59], que en la Constitución Española aparece en el artículo 15.
- **Vida familiar**: el Tribunal afirma que este precepto presupone la existencia de una familia, sin que sea necesario que exista convivencia en común para hablar de vida familiar entre padres e hijos menores. Se extiende también a otros vínculos existentes

[56] Art. 8.1 Convenio para la Protección de los Derechos Humanos… op. cit. p.17.

[57] RUIZ MIGUEL, C., *La configuración constitucional del derecho a la intimidad*. LUCAS VERDU, Pablo (dir.). Tesis doctoral, Universidad Complutense de Madrid, Departamento de Derecho Constitucional, 1995.

[58] STEDH 22 de octubre de 1981, as. C-7525/76, *Dudgeon vs. The United Kingdom*

[59] STEDH 26 de marzo de 1985, as. C-8978/80 *X and Y vs. The Netherlands*

con diversos parientes, fundamentalmente entre abuelos y nietos, cuya importancia resalta el Tribunal[60].

- **Respeto de la correspondencia**: dado que la expresión en muy concisa, el TEDH ha realizado una interpretación extensiva y finalista de la norma, es decir, se ha basado en lo que ésta pretende proteger, y también sociológica, en el sentido de que ha tenido en cuenta las circunstancias sociales, y sobre todo sus cambios, en el momento de redacción y a lo largo de los años. En la Sentencia Klass y otros contra Alemania, el Tribunal establece por primera vez que las escuchas telefónicas se encuentran comprendidas en el concepto de "vida privada". En sentencias posteriores va más allá, entendiendo que la detección y grabación de números que han sido marcados, junto con la hora o la duración de cada llamada, también constituyen una información que las autoridades no deben conocer sin causa legítima[61]. Asimismo, en la sentencia Weber y Saravia contra Alemania, el Tribunal establece que "*las nociones "vida privada" y "correspondencia" incluyen también las comunicaciones por teléfono, fax y correo electrónico*"[62].

3.2. Límites

La cuestión sobre los límites del artículo 8.1 del Convenio ha sido abordada en diversas ocasiones por el Tribunal, sobre todo en lo relativo al segundo párrafo de este mismo artículo, que dice lo siguiente:

> "*No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y de las libertades de los demás*"[63].

En definitiva, el Convenio admite que el Estado pueda interferir en la vida privada y en las comunicaciones de sus ciudadanos, pero siempre que se cumplan tres requisitos fundamentales, que se han ido confirmando en sucesivas sentencias:

---

[60] STEDH 13 de junio de 1979, as. C-6833/74 *Marckx vs. Belgium* ; STEDH 18 de diciembre de 1986, as. C-9697/82, *Johnston and others vs. Ireland*

[61] STEDH 2 de agosto de 1984, as. C-8691/79 *Malone vs. The United Kingdom*

[62] STEDH 29 de junio de 2006, as. C-54934/00 *Weber and Sarabia vs. Germany* (77).

[63] Art. 8.2 Convenio para la Protección de los Derechos Humanos…op.cit. p.17.

- Previsión legal.
- Finalidad legítima.
- Necesidad en una sociedad democrática.

En la sentencia Klass y otros contra Alemania (1978), que versa sobre la restricción del secreto de correspondencia, envíos postales y telecomunicaciones, el Tribunal no distingue con tanta claridad como las venideras estos tres requisitos al examinar la cuestión de si se ha violado el artículo 8 del Convenio. Sin embargo, sienta los parámetros que posteriormente se instaurarían, pues en primer lugar examina si la legislación comprobada justifica adecuadamente la injerencia. Señala que sólo la protección de la democracia ampara que los Estados puedan vigilar a sus ciudadanos sin su previo consentimiento; de lo contrario, estarían abriendo las puertas a convertirse en nada menos que Estados policíacos. Por tanto, al Tribunal le preocupa enormemente el alcance de la vigilancia, aún justificada, pues el Estado se convertiría en una suerte de policía suprema.

A) Prevista por la ley

Este requisito de previsión legal comprende a su vez dos elementos, necesarios ambos para que se entienda que la injerencia del Estado es aceptable y no punible: existencia de una base legal y calidad de la ley. Así se especifica en diversas sentencias como la del caso Malone[64] y el caso Kruslin contra Francia[65]. En esta última el Tribunal sistematiza también de forma sencilla cuáles son las características que debe tener la ley del Derecho interno para que pueda considerarse "de calidad".

Respecto a la primera cuestión, la existencia de una base legal en el Derecho interno, en el caso Silver y otros[66] el Tribunal entiende que las palabras "prevista por la ley" del artículo 8.2 del Convenio deben interpretarse en el sentido de lo recogido por la sentencia Sunday Times[67]. En esta sentencia el Tribunal acepta que la palabra "ley" comprende tanto el derecho escrito como el consuetudinario, e incluso debe atenderse también a la jurisprudencia. En cuanto a la consideración de la jurisprudencia, el caso Sunday Times se enmarcaba en el sistema de *common law*, pero aún así el Tribunal entiende en el caso Kruslin que la jurisprudencia toma un papel relevante también en los países

[64] STEDH 2 de agosto de 1984, as. C-8691/79 *Malone vs. The United Kingdom*
[65] STEDH 24 de abril de 1990, as. C-11801/85, *Kruslin vs. France*
[66] STEDH 25 de marzo de 1983, as. 5947/72 *Silver and others vs. The United Kingdom* (85)
[67] STEDH 26 de abril de 1979, as. C-6538/74 *The Sunday Times vs. The United Kingdom*

"continentales", "*hasta el punto de que todas las ramas del Derecho positivo son resultado, en buena parte, de las resoluciones de los Jueces y tribunales"*[68].

En cuanto a la segunda cuestión, la calidad de la ley, las sentencias Kruslin y Huvig marcan una serie de exigencias que dicha ley debe reunir, en concreto su accesibilidad y su previsibilidad conforme a la preeminencia del Derecho. Se entiende que una ley es accesible cuando los ciudadanos disponen de suficiente información acerca de qué normas jurídicas son aplicables a un caso concreto. Además, es necesario que la ley, para que pueda ser considerada como tal, se exprese de forma que los individuos puedan ajustar su comportamiento y prever razonablemente las consecuencias de éste.

En el caso de la interceptación de las comunicaciones, no implica que todos los ciudadanos deban poder prever si y cuando sus comunicaciones corren el riesgo de interceptarse por las autoridades para que puede actuar en consecuencia, sino que significa que la ley debe ser lo suficientemente transparente como para que cada individuo pueda tener la certeza de cuándo, por qué y cómo se permite la utilización de estas medidas[69].

Además, la ley debe fijar también su alcance, con un grado de precisión que dependerá de la materia de que se trate[70], puesto que de no ser así la ley pugnaría con la supremacía del derecho. En la sentencia Valenzuela contra España, el Tribunal desarrolla unas garantías mínimas necesarias para evitar los abusos de poder: "*la definición de las categorías de personas cuyas líneas telefónicas pueden ser intervenidas por orden judicial; la naturaleza de los delitos que pueden dar lugar a dicha orden judicial; la duración máxima de la ejecución de la medida; el procedimiento de transcripción resumida de las conversaciones interceptadas; las precauciones a adoptar para comunicar las grabaciones realizadas intactas y completas a los efectos del eventual control por el Juez y por la defensa; y, las circunstancias en las que se puede o se debe proceder al borrado o a la destrucción de las cintas, en especial, después de un sobreseimiento o de una absolución"*[71].

B) Finalidad legítima y necesidad en una sociedad democrática

Este requisito apenas ha tenido desarrollo jurisprudencial por parte del Tribunal Europeo de Derechos Humanos, que se suele limitar a determinar si la injerencia se

[68] STEDH 24 de abril de 1990, as. C-11801/85, *Kruslin vs. France* (29:2).
[69] STEDH 2 de agosto de 1984, as. C-8691/79 *Malone vs. The United Kingdom*(67).
[70] STEDH 2 de agosto de 1984, as. C-8691/79 *Malone vs. The United Kingdom* (68).
[71] STEDH 30 de julio de 1998, as. C-27671/95 *Valenzuela Contreras vs. Spain* (59).

encuentra amparada por alguna de las finalidades del artículo 8.2 del Convenio. Este artículo dice que son fines legítimos los previstos como límites en el apartado anterior, y que son fundamentalmente los que amenazan más gravemente la integridad democrática de los Estados.

El Tribunal acepta que el hecho de que la delincuencia haya aumentado en los últimos tiempos supone que los Estados deben contrarrestarla de alguna manera, por ejemplo con medidas de intervención telefónica que ayuden en la investigación y la lucha contra los delitos, especialmente los cometidos de forma organizada. Pero el riesgo de que se abuse de este poder es evidente, lo cual crearía consecuencias perjudiciales para una sociedad democrática. Por eso, entiende el Tribunal, que la intervención sólo se considera necesaria si el sistema incorpora garantías suficientemente protectoras frente a los abusos[72].

En el asunto Weber y Sarabia, el Gobierno alemán justificó la necesidad de la ley en el combate contra el terrorismo internacional, en especial para desactivar al grupo Al-Qaeda tras los atentados del 11 de septiembre.

3.3. El asunto Liberty y otros contra Reino Unido

Tiene su origen en una demanda presentada por Liberty, British Irish Rights Watch e Irish Council for Civil Liberties, contra Reino Unido e Irlanda del Norte. Se trata de tres organizaciones (una británica y dos irlandesas) que tratan de velar por la protección y respeto de las libertades civiles.

Las demandantes alegaban que en los años 90 el Ministerio de Defensa inició una "Utilidad de Prueba Electrónica" en Cheshire, con el objetivo de interceptar 10.000 canales telefónicos simultáneos desde Dublín a Londres y al continente. Era capaz de interceptar todas las telecomunicaciones públicas (teléfono, fax, correo electrónico, etc.) mantenidas por radio entre las dos emisoras de British Telecom, que en aquel momento soportaba la mayor parte del tráfico de telecomunicaciones de Irlanda. Tras conocer estos hechos, las demandantes solicitaron al Tribunal de Intervención de Comunicaciones (ICT, por sus siglas en inglés) que investigara la legalidad de cualquier orden que hubiera podido emitirse respecto a sus comunicaciones; el Tribunal les respondió que, en virtud de la Ley de 1985 (*Interception of communications act 1985*) no podía conocer antes de investigar si existe alguna orden dictada para un caso concreto. Además, una vez investigado el caso en concreto, el Tribunal no podía revelar si se había producido o no

[72] STEDH 2 de agosto de 1984, as. C-8691/79 *Malone vs. The United Kingdom* (81).

la interceptación de las comunicaciones en el caso de que dicha interceptación no violara lo dispuesto por la Ley.

Esta ley establecía una serie de excepciones a la interceptación de comunicaciones, que de no darse constituiría un delito: seguridad nacional, prevención y detección de delitos graves o salvaguardar el bienestar económico del Reino Unido.

El término "delitos graves" debía entenderse en aquellos casos en que la conducta implicara el uso de la violencia, tuviera como resultado una ganancia económica sustancial, fuera llevada a cabo por un amplio número de personas en busca de un objetivo común, o cuya pena fuese de al menos tres años de prisión.

Por seguridad nacional entendemos el conjunto de actividades o actos que suponen una amenaza para el Estado, y cuyo propósito puede ser hacer tambalear o incluso tumbar la democracia parlamentaria. Los medios que se valen aquellos que amenazan la seguridad nacional pueden ser de diferentes tipos, incluidos los políticos, los industriales o también la violencia.

La orden de interceptación de las comunicaciones debía ser emitida por el *Secretary of State*, que tenía la obligación de observar si la información a obtener podía ser obtenida razonablemente por otros medios. Además, las órdenes para proteger el bienestar económico del Reino Unido no podían dictarse a menos que la información a obtener tuviese relación con actos o intenciones de personas que se encontrasen fuera de las Islas Británicas.

El artículo 3 permitía dos tipos de órdenes de interceptación. En primer lugar, las de comunicaciones enviadas a o desde uno o más domicilios especificados en la orden, siendo el domicilio o los domicilios probables a utilizar para la transmisión de comunicaciones a o de una persona determinada especificada en la orden o una serie determinada de instalaciones. En segundo lugar, las de interceptación del sistema público de interceptaciones, que permitiría captar telecomunicaciones externas tal y como se describieran en la orden y otras comunicaciones si fuera necesario interceptarlas. Tras esto, el *Secretary of State* debía emitir un certificado describiendo el material interceptado. En tercer lugar, las consideradas necesarias para prevenir o detectar actos de terrorismo.

El artículo 6 contenía las "salvaguardias" que debían asegurarse. Fundamentalmente se refiere a la determinación de las personas y comunicaciones concretas a que debía afectar la orden y a la limitación del material divulgado, el número de personas a las que

se divulga, el material copiado y el número de copias hechas, al mínimo necesario. Además, las copias debían destruirse en cuanto su conservación ya no fuera necesaria.

El artículo 7 establecía que el ICT debía limitarse a comprobar la adecuación a la ley de la orden cursada, que de confirmarse le imposibilitaría informar al interesado de la efectiva interceptación de sus comunicaciones. Solamente cuando la orden no se adecuaba a lo previsto por esta ley se autorizaba al Tribunal a confirmar la efectuación de la interceptación.

El artículo 8 preveía la creación de un Comisionado encargado de controlar la actuación del *Secretary of State*, proporcionar al ICT la asistencia que requiriese, controlar la idoneidad de las medidas adoptadas para proteger el material y destruirlo cuando no fuera necesaria su conservación, informar al Primer Ministro cuando pudiera haber una violación o se llevasen a cabo medidas inadecuadas, y elaborar un informe anual.

Esta ley estuvo vigente hasta el año 2000, cuando se promulgó la Ley de Regulación de las facultades de investigación (*The Regulation of Investigatory Powers Act 2000*), que derogó los artículos 1 a 10 de la ley de 1985, estableciendo un nuevo régimen para la intervención de las telecomunicaciones.

Cuando se presentó la demanda, la ley en vigor era la de 1985, por lo que el Tribunal Europeo de Derechos Humanos emitiría su resolución el año 2008 en base a lo dispuesto por ésta. En sus alegaciones, los demandantes expusieron que las órdenes de interceptación no identificaban objetivos ni domicilios concretos, y que tampoco requerían ser más específicos que los tipos amplios que preveía la ley (seguridad nacional, prevención de delitos graves o protección del bienestar económico del Reino Unido. Tampoco se especificaban los términos de búsqueda o los criterios de filtrado utilizados por los funcionarios del Estado, que además no consultaban a funcionarios judiciales o ministros. Y respecto a la protección de aquellos a los que se les hubieran intervenido las comunicaciones, solamente se proporcionaban las "medidas necesarias a efectos de asegurar que ninguna persona lea, examine o escuche el material no incluido en el certificado", pero el carácter preciso de estas medidas no era público, ni existía ningún procedimiento que permitiese a la persona convencerse de que se habían cumplido.

En su contestación, el Gobierno alegó que la divulgación de las medidas revelaría información importante sobre los métodos de interceptación utilizados, por lo que no puede revelar todos los detalles de las medidas adoptadas. Señaló que el Tribunal debería partir de la base de que, a falta de pruebas de lo contrario, en la sociedad democrática del

Reino Unido los ministros, funcionarios y Comisionados desempeñan adecuadamente sus funciones reglamentarias para asegurar que se establezcan las garantías exigidas por la ley. Afirmó también que el régimen relativo a la orden era proporcional y necesario en una sociedad democrática porque los Estados se enfrentaban a la creciente amenaza del terrorismo y en la medida en que aumenta el alcance y la sofisticación de las redes de comunicaciones, las organizaciones terroristas han adquirido el mayor ámbito de funcionamiento y cooperación a nivel transnacional.

Visto lo anterior, el Tribunal entiende que la injerencia en el artículo 8.1 del Convenio está justificada en base al segundo apartado del mismo artículo. Pero arguyen que la Ley de 1985 no era lo suficientemente detallada ni precisa para cumplir la exigencia de "previsibilidad" porque la naturaleza de las medidas adoptadas en virtud de la misma no era accesible al público.

Dice el Tribunal que "*la previsibilidad no significa que una persona pueda prever cuándo es probable que las autoridades intercepten sus comunicaciones para adaptar su comportamiento en consecuencia*"[73]. Sin embargo, especialmente cuando la facultad conferida al Ejecutivo se ejerce en secreto, el riesgo de actos arbitrarios es evidente. Por tanto, es esencial tener unas normas claras y detalladas para la interceptación de conversaciones telefónicas, "*tanto más cuanto que los procedimientos técnicos no cesan de perfeccionarse. El Derecho interno ha de emplear términos suficientemente claros para indicar a todos de manera suficiente en qué circunstancias y bajo qué condiciones habilita a los poderes públicos a tomar tales medidas.*

La Ley pugnaría con la supremacía del derecho de que se trata si la facultad discrecional concedida a la Administración no tuviera límites. Por tanto, la Ley ha de indicar el alcance y las modalidades de ejercicio de dicha facultad con suficiente claridad para facilitar así al individuo la adecuada protección contra las injerencias arbitrarias"[74].

Recuerda el Tribunal que la Ley de 1985 concede al Ejecutivo una amplia facultad respecto a la intervención de las telecomunicaciones entre el Reino Unido y un receptor externo. No existía ningún límite en cuanto al conjunto de comunicaciones procedentes del exterior sobre las que podría dictarse una orden. La facultad discrecional conferida al Ejecutivo para la interceptación física de este tipo de comunicaciones era, por tanto, prácticamente ilimitada.

[73] STEDH 1 de julio de 2008, as C-58243/00 *Liberty and Others vs. The United Kingdom* (62).
[74] Ídem.

El Tribunal también hace suya la alegación de los demandantes respecto a que la legislación no contenía los detalles de las medidas adoptadas en virtud del artículo 6, ni se hacían públicos.

Por tanto, el Tribunal entiende que el sistema para la intervención de las comunicaciones externas en virtud de la Ley de 1985 no había sido expresado de forma suficientemente clara y precisa, de manera que los ciudadanos no resultaban protegidos frente a injerencias injustificadas.

4. El secreto de las comunicaciones en España: adaptación de la LECrim a la jurisprudencia del TEDH

En España el secreto de las comunicaciones se protege en su Ley Fundamental desde mediados del siglo XIX, permaneciendo todavía vigente en la Constitución de 1978, en vigor actualmente. Las Constituciones de 1869[75] y 1876[76] se pronunciaban en términos bastante similares en sus artículos 7 y 8; en ellos, se prohibía a la Autoridad gubernativa que detuviera o abriera la correspondencia confiada al correo, como tampoco la telegráfica salvo auto judicial motivado. Que se haga referencia al correo escrito y telegráfico como únicos medios objeto de interceptación responde a la imprevisión de los futuros avances técnicos en el campo de las telecomunicaciones. Estos avances ya se habían comenzado a extender al tiempo de redacción de la Constitución republicana de 1931[77], que también reconoce en su artículo 32 la inviolabilidad de la correspondencia en todas sus formas salvo auto judicial en contrario.

---

[75] Art. 7 de la Constitución española de 1869: "En ningún caso podrá detenerse ni abrirse por la Autoridad gubernativa la correspondencia confiada al correo, ni tampoco detenerse la telegráfica. Pero en virtud de auto del juez competente podrán detenerse una y otra correspondencia, y también abrirse en presencia del procesado la que se le dirija por correo."

Art. 8 de la Constitución española de 1869: "Todo auto de prisión, de registro de morada, o de detención de la correspondencia escrita o telegráfica, será motivado. Cuando el auto carezca de este requisito, o cuando los motivos en que se haya fundado se declaren en juicio ilegítimo o notoriamente insuficientes, la persona que hubiere sido presa, o cuya prisión no se hubiere ratificado dentro del plazo señalado en el art. 4º., o cuyo domicilio hubiere sido allanado, o cuya correspondencia hubiere sido detenida, tendrá derecho a reclamar del juez que haya dictado el auto una indemnización proporcionada al daño causado, pero nunca inferior a 500 pesetas."

Disponible en: http://www.congreso.es/constitucion/ficheros/historicas/cons_1869.pdf

[76] Art. 7 de la Constitución española de 1876: "No podrá detenerse ni abrirse por la autoridad gubernativa la correspondencia confiada al correo."

Art. 8 de la Constitución española de 1876: "Todo auto de prisión, de registro de morada o de detención de la correspondencia, será motivado."

Disponible en: http://www.congreso.es/constitucion/ficheros/historicas/cons_1876.pdf

[77] Art. 32 de la Constitución española de 1931: Queda garantizada la inviolabilidad de la correspondencia en todas sus formas, a no ser que se dicte auto judicial en contrario.

A continuación, tenemos la Constitución de 1978[78], elaborada ya en periodo democrático tras la caída del régimen franquista, que en su artículo 18.3 garantiza el secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas, también salvo resolución judicial. Sin embargo, este artículo por sí sólo no es suficiente, sino que precisa de desarrollo a través de una Ley Orgánica, que es aquella que es aprobada por mayoría absoluta en las Cortes. No sería hasta 1988 que se promulgó la Ley Orgánica 4/1988[79] de 25 de mayo, que modificó el artículo 579 de la Ley de Enjuiciamiento Criminal (LECrim). Antes de esta modificación la intervención se llevaba a cabo con base en el artículo 18.3 de la Constitución y el antiguo artículo 579 de la LECrim, hasta que el Tribunal Europeo de Derechos Humanos en el caso Valenzuela contra España declaró que la interceptación requería de una ley de calidad con los requisitos anteriormente señalados.

Sin embargo, esta nueva regulación tampoco se mantendría demasiado tiempo, puesto que en 2003 una nueva sentencia del TEDH (caso Prado Bugallo contra España) entendió que las garantías introducidas por la Ley Orgánica de 1988 no respondían a todas las condiciones exigidas en su jurisprudencia. Esta ley no determinaba los delitos que permitían las escuchas; tampoco un límite temporal en la duración de la interceptación; tampoco regulaba las condiciones que debían cumplirse para asegurar la regularidad de las escuchas ni las precauciones a tomar para conservar intactas y completas las comunicaciones interceptadas. Tras esta sentencia, nuestros tribunales se encargaron de generar a través de su jurisprudencia los requisitos mínimos que debían cumplir las intervenciones telefónicas para ajustarse a la legalidad, hasta alcanzar finalmente la aprobación del TEDH. No obstante, no deja de ser llamativo que haya sido a través del desarrollo jurisprudencial que se regulara una materia que desde un primer momento correspondía al legislador. Así queda claro que nuestro sistema procesal adolece de ciertos problemas, que implican una deficiente calidad en relación con lo que se espera de una democracia. Así fue señalado reiteradamente por la doctrina, tal y como indica el preámbulo de la LO 13/2015[80].

Disponible en: http://www.congreso.es/constitucion/ficheros/historicas/cons_1931.pdf

[78] Art. 18.3 Constitución española de 1978: Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

[79] ESPAÑA. Ley Orgánica 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal. *BOE* núm. 126, de 26 de mayo de 1988, pp. 16159 a 16160.

[80] ESPAÑA. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las

La LO 13/2015 introdujo en la LECrim[81] una regulación exhaustiva de la intervención de las comunicaciones telefónicas y telemáticas como diligencia de investigación que limita el derecho fundamental del art.18CE. Lo hace en el Capítulo V del Título VIII del Libro II, artículos 588 ter a) a 588 ter m). Es en este título donde se regulan todas las medidas que limitan el derecho fundamental al secreto de las comunicaciones junto con el resto de los derechos del mismo precepto constitucional.

Los que interesan a efectos del presente trabajo para determinar la posibilidad de que en España se pueda realizar una interceptación de comunicaciones son los Capítulos IV a VI, aunque las Disposiciones Comunes del primero de ellos son aplicables también a los siguientes. Estudio separado merece lo dispuesto acerca de esta cuestión en otras leyes que permiten la interceptación de comunicaciones que no obedezcan a la causa ordinaria de instrucción de causas penales. Esto se debe a que circunstancias diferentes requieren también medidas diferentes, contempladas en la LO 2/2002 reguladora del control judicial previo del CNI o en la LO 4/1981 de los estados de alarma, excepción y sitio.

En los últimos años, la jurisprudencia ha ido delimitando el ámbito de protección constitucional para las comunicaciones. El Tribunal Supremo, el Tribunal Constitucional y el Tribunal Europeo de Derechos Humanos han señalado cuáles y cómo son las comunicaciones que merecen tal protección; algunas de ellas ya se han mencionado anteriormente, como las Sentencias Malone contra Reino Unido y Copland contra Reino Unido, en relación con los datos externos como la identidad de los interlocutores, el registro de llamadas o la misma realización de la comunicación entre sujetos, incluyendo el momento, duración y destino. En cambio, la previsión constitucional no alcanza a las conversaciones grabadas o difundidas por uno de los interlocutores[82]. Tampoco las comunicaciones por radio[83], el visionado de un número de teléfono entrante[84] ni "*la conversación escuchada por agentes policiales a través del manos libres de uno de los interlocutores que accede a ello*"[85].

---

medidas de investigación tecnológica. *BOE* núm. 239, de 6 de octubre de 2015, pp. 90192 a 90219.

[81] ESPAÑA. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. *BOE* núm. 260, de 17 de septiembre de 1882.

[82] SSTC nº 175/2000, de 26 de junio; 56/2003, de 24 de marzo; STS nº 421/2014, de 16 de mayo.

[83] SSTS nº 209/2007, de 9 de marzo; 1397/2011, de 22 de diciembre; 695/2013, de 22 de julio.

[84] SSTS nº 1040/2005, de 20 de septiembre; 1273/2009, de 17 de diciembre.

[85] STS nº 589/2015, de 28 de septiembre.

El artículo 588 bis da comienzo al Capítulo IV, de las Disposiciones Comunes, y establece que durante la instrucción de las causas se podrá acordar la intervención de las comunicaciones mediante autorización judicial, que debe sujetarse a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

Para entender que una medida cumple el principio de especialidad, tiene que estar asociada a un delito concreto. Por tanto, no es posible adoptar medidas de investigación relacionadas con la intervención de comunicaciones con el objetivo de prevenir delitos de los que no existan indicios o no se pueda probar la existencia de sospechas fundadas objetivamente.

Este principio se concreta en el artículo 588 ter a., el primero relativo específicamente a la interceptación de las comunicaciones telefónicas y telemáticas. Supone que solamente se podrán autorizar las intervenciones telefónicas y telemáticas cuando estén relacionadas con los delitos contenidos en el artículo 579.1 de la LECiv, o aquellos que hayan sido cometidos mediante técnicas o tecnología informáticas o de la comunicación. Los delitos que recoge el artículo 579.1 son, en primer lugar, los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; en segundo lugar, delitos cometidos en el seno de un grupo u organización criminal; y en tercer lugar, tal y como han hecho otros muchos países tras los sucesos ocurridos en las últimas décadas en Occidente, los delitos de terrorismo.

Se trata de un abanico muy amplio, dado que los delitos cuya pena máxima es de al menos tres años de prisión no son pocos. El requisito adicional de que se trate de delitos dolosos implica que debe existir una intencionalidad subjetiva de producir el daño. Por otro lado, el artículo 570 bis de la LO 10/1995, de 23 de noviembre, del Código Penal[86], señala que "*se entiende por organización criminal la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan tareas o funciones con el fin de cometer delitos*"[87]. A continuación, el artículo 570 ter 1 párrafo segundo, define como grupo criminal "*la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal, tenga por finalidad o por objeto la perpetración concertada de delitos*"[88].

[86] ESPAÑA. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *BOE* núm. 281, de 24 de noviembre de 1995.

[87] Art.570 bis Ley Orgánica 10/1995, op. cit.

[88] Art.570 ter Ley Orgánica 10/1995…op. cit. p. 32.

En cuanto a los delitos conexos, la Circular 1/2019 de la Fiscal General del Estado expone que "*la intervención telefónica o telemática está justificada cuando se fundamente en el delito principal, de manera que no existe inconveniente para valorar y considerar el delito conexo casualmente hallado, pero nunca podrá acordarse ni prorrogarse la medida con fundamento en el delito conexo si desaparece el delito que la justifica*"[89].

Esta Circular señala también que "*el principio de especialidad prohíbe por sí mismo la adopción de una medida de investigación prospectiva que limite los derechos fundamentales*"[90]. Tal y como señala la STS nº 195/2010, de 28 de enero, la medida "*debe delimitarse objetivamente a través de la precisión del hecho que se trata de investigar, y subjetivamente mediante la suficiente identificación del sospechoso*"[91].

Además del criterio objetivo que implica el principio de especialidad, deben darse juntamente con éste otras características específicas para que la medida de interceptación de comunicaciones sea admisible. Según el principio de idoneidad, es necesario indicar los ámbitos de aplicación de las medidas, tanto objetivo como subjetivo, y su duración. El artículo 588 quater b 2.b puntualiza en este sentido que la idoneidad puede venir referida a la previsión racional de aportación de *"datos esenciales y de relevancia probatoria para el esclarecimiento de los hechos y la identificación de su autor*"[92]. Es decir, una medida es idónea cuando hay indicios suficientemente racionales para creer que es adecuada para el objetivo a que se destina, que es la resolución de un delito. Así lo corroboran tanto el Tribunal Supremo como el Tribunal Constitucional en diversas sentencias, como por ejemplo las SSTS nº 85/2017, de 15 de febrero y 993/2016, de 12 de enero de 2017; y la STC nº 207/1996, de 16 de diciembre).

Continúa la Circular 1/2019 exponiendo que en virtud del principio de excepcionalidad y necesidad "*sólo podrá acordarse la medida cuando no se puedan adoptar otras medidas menos gravosas para los derechos fundamentales del investigado e igualmente útiles; y cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización*

[89] ESPAÑA. Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal. *BOE* núm. 70, de 22 de marzo de 2019, pp. 30061 a 30090.

[90] Ídem.

[91] STS nº 195/2010, de 28 de enero.

[92] Art. 588 quater b 2 apartado b Ley de Enjuiciamiento Criminal, op. cit. p. 31

de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida"[93]. El principio de necesidad es uno de los presupuestos esenciales a que se refieren el artículo 8.2CEDH y la jurisprudencia del TEDH, como es la necesidad en una sociedad democrática de la medida adoptada.

Por su parte, para que una medida cumpla el principio de proporcionalidad, los derechos e intereses que se vean afectados por su adopción lo estarán en un grado inferior al beneficio que aporte a la colectividad en general o a terceros en particular. Para ello se tendrán en cuenta algunos parámetros como la gravedad del hecho investigado, la importancia que la sociedad le otorgue subjetivamente, su relevancia dentro del ámbito tecnológico, la magnitud de los indicios recabados que permitan suponer el perjuicio; y sobre todo, será de gran importancia que con la medida adoptada pueda lograrse satisfactoriamente un resultado eminentemente positivo que justifique la adopción de la medida y la limitación de los derechos.

Respecto del ámbito objetivo, el artículo 588 ter b dispone que "*comprende el contenido de las comunicaciones y los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado. También se pueden intervenir los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad*"[94]. Sin embargo, será el Juez quien deba concretar el alcance de la intervención, siempre justificando y fundamentando la necesidad de una mayor amplitud de la medida en base a los principios rectores anteriormente examinados. El artículo 588 ter d añade a estos requisitos, otros tantos que debe contener la solicitud de autorización judicial: "*la identificación del número de abonado, del terminal o de la etiqueta técnica; la identificación de la conexión objeto de la intervención; o los datos necesarios para identificar el medio de telecomunicaciones de que se trate*"[95]. Y refiriéndose al contenido, su apartado segundo precisa que, "*para determinar la extensión de la medida, la solicitud de autorización judicial puede tener por objeto:*

a) *El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta.*

[93] Ibídem p.32
[94] Art. 588 ter b Ley de Enjuiciamiento Criminal, op. cit. p.31
[95] Art. 588 ter d Ídem.

b) *El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza.*
c) *La localización geográfica del origen o destino de la comunicación.*
d) *El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación*"[96].

En cuanto al ámbito subjetivo, está regulado en los artículos 588 ter b y c. En primer lugar se incluyen los terminales o medios de comunicación habitual u ocasionalmente utilizados por el investigado; y en segundo lugar, se posibilita la intervención judicial de terminales o medios telemáticos de terceros, pero para ello debe acreditarse que la persona investigada los utiliza, ya sea para emitir o recibir información, o si el titular colabora con ella o se beneficia de su actuación admite. Por tanto, no es tan importante la titularidad del medio que se utilice para la comunicación como que sea el sujeto investigado quien participe de ella, bien sea personalmente como a través de un tercero que colabora con él, o que incluso es ajeno. Sin embargo, y para salvaguardar especialmente los derechos de estos terceros, la adopción de la medida que limite sus derechos fundamentales de esta forma requerirá una especial motivación por parte del juez, que cumpla de manera taxativa con el principio de idoneidad. En último término, se podrán intervenir también los de la víctima cuando se ponga de relieve un riesgo grave para su vida o integridad.

A continuación, el artículo 588 ter e impone una obligación a todas las compañías que presten servicios de telecomunicaciones, de acceso a una red o de servicios de la sociedad de la información. Ésta es la de prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial la asistencia y colaboración necesarias para el cumplimiento de la intervención, debiendo además guardar secreto acerca de lo requerido por las autoridades, bajo pena de delito de desobediencia. Dada la amplitud de las redes de comunicaciones y servicios de la información, se pueden plantear algunos problemas de jurisdicción en relación con aquellos que radican fuera de las fronteras españolas. La necesidad de remitir o no la solicitud de interceptación a través de una comisión rogatoria u orden europea de investigación, vendrá determinado por la radicación o no del servicio en España. Se entiende que el servicio está establecido en España, según el artículo 2LSSICE[97], "cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y

[96] Art. 588 ter d apartado 2 Ley de Enjuiciamiento Criminal, op. cit. p.31
[97] ESPAÑA. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. *BOE* núm. 166, de 12 de julio de 2002.

la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección. Asimismo, será de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España". Además del criterio utilizado del establecimiento permanente situado en España, este mismo artículo prevé también las sucursales inscritas en el Registro Mercantil o cualquier otro registro público español en el que fuera necesaria la inscripción para adquirir personalidad jurídica.

No debemos olvidar tampoco el absolutamente necesario control que debe llevar la ejecución de una medida como esta, que afecta a derechos fundamentales. En este caso es el artículo 588 ter f el que obliga a la Policía Judicial a entregar al Juez las transcripciones de aquellos puntos de las conversaciones obtenidas a través de la intervención que sean relevantes para la investigación, indicando no sólo su origen y su destino, sino que también deberá señalares concretamente, a través de diferentes sistemas prestablecidos de aseguramiento de la autenticidad de lo obtenido, el soporte electrónico a través del cual se hubiera realizado la grabación.

En cuanto a la duración de las medidas y sus posibles prórrogas, el artículo 588 ter g establece como duración máxima inicial tres meses desde la fecha de autorización judicial, siendo prorrogables por periodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses. Para solicitar dichas prórrogas, la Policía Judicial deberá aportar la transcripción de los pasajes de las conversaciones de los que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida. A continuación, la ley admite la posibilidad de que el juez pueda solicitar aclaraciones o una cantidad mayor de información acerca de cómo se está desarrollando la investigación.

Por último, el artículo 588 ter i regula la entrega a las partes involucradas una copia de las grabaciones y transcripciones realizadas, salvo que hubiera en ellas referencias a aspectos íntimos de la persona, que se omitirán, una vez que haya expirado la vigencia de la medida, o cuando se haya alzado el secreto. Antes de que transcurra el plazo fijado por el juez, cualquiera de ellas puede solicitar la inclusión de otras comunicaciones que consideren relevantes y no hayan sido incluidas. El último apartado de este artículo regula un aspecto muy importante, que es la notificación a las personas intervinientes en las comunicaciones interceptadas, del hecho mismo de haber practicado la intervención, junto con la identificación expresa de las comunicaciones concretas que hayan resultado afectadas, siempre y cuando dicha notificación no sea imposible, no exija un esfuerzo desproporcionado y no exista riesgo de perjudicar futuras investigaciones.

Lo dispuesto por la Ley de Enjuiciamiento Criminal en lo que a la interceptación de comunicaciones se refiere, está complementado por diversas circulares de la Fiscal General del Estado que datan de 2019. La primera de ellas, citada anteriormente, se refiere a las disposiciones comunes y a las medidas de aseguramiento de las diligencias de investigación tecnológicas. Los principios rectores sobre los que se deben asentar las medidas de interceptación son el eje central de este documento. En segundo lugar, específicamente para la interceptación telefónica y telemática de comunicaciones, se encuentra la Circular 2/2019, de 6 de marzo[98]. Este texto explica ampliamente las disposiciones contenidas en el Capítulo V del Título VIII del Libro II de la Ley de Enjuiciamiento Criminal. Resta únicamente argumentar si realmente estas disposiciones respetan la jurisprudencia del TEDH en materia de intervención de comunicaciones, acerca del artículo 8 del CEDH.

Como ya se ha explicado anteriormente, toda injerencia del Estado en el derecho al respeto a la correspondencia debe estar prevista por la ley y, siendo necesaria en una sociedad democrática, debe tener como finalidad "*la defensa de la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*"[99]. Además, el TEDH complementa esta disposición a través de su jurisprudencia estableciendo los requisitos que debe cumplir la ley a que hace referencia el precepto, para que se entienda que una medida está realmente "prevista por la ley" y es "necesaria en una sociedad democrática". Dice el Tribunal reiteradamente, que "*la ley debe emplear términos suficientemente claros para que puedan conocer en qué circunstancias y mediante qué requisitos permite el Poder Público hacer uso de esta medida*"[100]. Y ello teniendo en cuenta que, a pesar del aumento en las últimas décadas de determinados comportamientos contrarios a las bases democráticas de nuestra sociedad, la intervención solamente estará justificada si el sistema cuenta con las garantías necesarias y suficientes para prevenir los abusos de las autoridades públicas.

Más concretamente, las principales garantías que el sistema debe reunir para evitar los abusos y estimarse acorde con el Convenio, fueron señaladas por el Tribunal en sendas

[98] ESPAÑA. Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas. *BOE* núm. 70, de 22 de marzo de 2019, pp. 30091 a 30120.

[99] Art.8.2 Convenio para la Protección de los Derechos Humanos, op. cit. p.17

[100] STEDH 2 de agosto de 1984, as. C-8691/79 *Malone vs. The United Kingdom*(67).

sentencias precisamente en las que España se encontraba involucrada por su deficiente previsión legislativa. Se trata, como ya se ha mencionado, de la sentencia Valenzuela Contreras. En ella, el Tribunal señala algunos requisitos que deben reunir las legislaciones internas de los Estados: "*la definición de las categorías de personas cuyas líneas telefónicas pueden ser intervenidas por orden judicial; la naturaleza de los delitos que pueden dar lugar a dicha orden judicial; la duración máxima de la ejecución de la medida; el procedimiento de transcripción resumida de las conversaciones interceptadas; las precauciones a adoptar para comunicar las grabaciones realizadas intactas y completas a los efectos del eventual control por el Juez y por la defensa; y, las circunstancias en las que se puede o se debe proceder al borrado o a la destrucción de las cintas, en especial, después de un sobreseimiento o de una absolución*.[101]"

Todas ellas se encuentran recogidas, como ya se ha señalado, entre los Capítulos IV y V del Título VIII de la Ley de Enjuiciamiento Criminal, con una regulación pormenorizada que efectivamente permite la interceptación de las comunicaciones en los casos previstos. Sin embargo, debe tenerse muy presente que uno de los principios informadores más importantes de este tipo de medidas, el principio de especialidad, impide la adopción prospectiva de medidas que vulneren el derecho fundamental al secreto de las comunicaciones, muy ligado al derecho a la intimidad. Es absolutamente necesaria, por tanto, la delimitación objetiva, subjetiva y temporal de medidas de este tipo. Parece impensable, al amparo de lo aquí relatado, la posibilidad de que en nuestro país se lleve a cabo una interceptación masiva de comunicaciones sin ningún tipo de control democrático.

4.1. Supuestos legales especiales

Además de los supuestos previstos por la Ley de Enjuiciamiento Criminal para la interceptación de comunicaciones, nuestro ordenamiento prevé otros que tienen un carácter especial. La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, en su artículo 4, apartado 6, señala que "*El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas en determinados supuestos excepcionales que puedan afectar al orden público, la seguridad pública y la seguridad nacional. En concreto, esta facultad excepcional y transitoria de*

[101] STEDH 30 de julio de 1998, as. C-27671/95 *Valenzuela Contreras vs. Spain* (59).

gestión directa o intervención podrá afectar a cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer el orden público, la seguridad pública y la seguridad nacional"[102]. Y respecto del secreto de las comunicaciones, el artículo 39, apartado 2, obliga a los operadores a realizar las interceptaciones que se autoricen de acuerdo con el artículo 579 LECrim, ya visto, con la Ley Orgánica 2/2002[103], de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, y con otras normas con rango de ley orgánica.

4.1.1 El Centro Nacional de Inteligencia

En la exposición de motivos de esta ley orgánica se señala que su finalidad es "*establecer un control judicial de las actividades del Centro que afecten a los derechos fundamentales reconocidos en el artículo 18.2 y 3 de la Constitución*"[104]. Además, se reconoce paralelamente la necesidad de que la regulación española se ajuste a lo dispuesto en el Convenio Europeo para la Protección de los Derechos Humanos. Para ello es necesario regular cómo se nombrará al Magistrado del Tribunal Supremo que se dedicará en exclusiva a controlar las actividades del CNI, y a través de qué procedimiento deberá este Magistrado autorizar o denegar tales actividades. Por último, señala esta exposición de motivos que el plazo para su acuerdo es de setenta y dos horas, que por motivos de urgencia debidamente justificados se puede reducir a veinticuatro horas.

En su breve articulado, pues solamente consta de un artículo, una disposición adicional y una disposición final, esta ley presenta los requisitos que debe reunir la solicitud de autorización para la adopción de medidas de interceptación de comunicaciones por el Centro, y que no difieren en exceso de lo regulado en la Ley de Enjuiciamiento Criminal:

"*La solicitud de autorización se formulará mediante escrito que contendrá los siguientes extremos:*

a) Especificación de las medidas que se solicitan.

b) Hechos en que se apoya la solicitud, fines que la motivan y razones que aconsejan la adopción de las medidas solicitadas.

[102] ESPAÑA. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. *BOE* núm. 114, de 10 de mayo de 2014.

[103] ESPAÑA. Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. *BOE* núm. 109, de 7 de mayo de 2002, pp. 16439 a 16440.

[104] Ídem.

c) *Identificación de la persona o personas afectadas por las medidas, si fueren conocidas, y designación del lugar donde hayan de practicarse.*

d) *Duración de las medidas solicitadas, que no podrá exceder de veinticuatro horas en el caso de afección a la inviolabilidad del domicilio y tres meses para la intervención o interceptación de las comunicaciones postales, telegráficas, telefónicas o de cualquier otra índole, ambos plazos prorrogables por sucesivos períodos iguales en caso de necesidad"*[105].

Además, el punto cuatro de su artículo único ordena "*la inmediata destrucción del material relativo a todas aquellas informaciones que, obtenidas mediante la autorización prevista en este artículo, no guarden relación con el objeto o fines de la misma*"[106].

A pesar de la relativa laxitud que parece recoger esta norma en relación a los supuestos que pueden ser objeto de medidas restrictivas de los derechos del art.18CE, no se entiende lo aquí recogido sin la observancia de la ley que regula las funciones y objetivos, y en definitiva el motivo de la propia existencia del Centro Nacional de Inteligencia. Por ello, la Ley 11/2002 señala en su artículo 1 que su principal cometido es "*la obtención de información y elaboración de análisis, estudios y propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones*"[107]. Parece entonces razonable entender entonces, que las injerencias en los derechos fundamentales de los ciudadanos por parte de este organismo se refieren únicamente a aquellas actuaciones que puedan poner en riesgo la salvaguarda de los pilares sobre los que se asienta la sociedad democrática española.

5. Conclusiones

La creación durante el siglo XX de sistemas de interceptación masiva de comunicaciones supuso una grave injerencia en la vida de los ciudadanos, que sin saberlo vieron afectados sus derechos fundamentales garantizados en las constituciones nacionales. A pesar de que su existencia se fue haciendo pública a los pocos años de su surgimiento, los Estados continúan desarrollando todo tipo de programas tratando de obtener datos sensibles sobre la población, que posteriormente analizan y comparten con

[105] Ibídem p.39.
[106] Ídem.
[107] ESPAÑA. Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. *BOE* núm. 109, de 7 de mayo de 2002.

otros servicios de inteligencia. Especialmente preocupante resulta la posible aplicación para el espionaje industrial de estas herramientas, que podrían afectar gravemente al sistema económico mundial.

Por ello, en todo el mundo se han ido elaborando diferentes instrumentos jurídicos vinculantes que tratan de obligar a los Estados a no llevar a cabo este tipo de prácticas, pero su capacidad para imponer sanciones y exigir responsabilidad de cualquier tipo está todavía demasiado mermada. La región en la que más se ha profundizado en este sentido es Europa, donde el Convenio Europeo para la Protección de los Derechos Humanos es la principal norma de referencia. En particular, su artículo 8 establece una serie de garantías que toda norma que autorice la interceptación de comunicaciones debe reunir; además, han sido desarrolladas fundamentalmente por la jurisprudencia del Tribunal Europeo de Derechos Humanos, creado por el mismo convenio para asegurar su cumplimiento y sancionar las infracciones al mismo. Desde entonces se han planteado múltiples asuntos a través de los cuales el Tribunal ha establecido los requisitos de previsibilidad, finalidad legítima y necesidad en una sociedad democrática.

Una norma es previsible cuando tiene una base suficiente en el Derecho interno, abarcando tanto las normas escritas como las consuetudinarias y la jurisprudencia de los órganos judiciales. Además, se refiere también a la "calidad" de la ley, en el sentido de que los ciudadanos deben disponer de suficiente información acerca de las normas jurídicas aplicables, y debe permitirles ajustar su conducta y prever razonablemente las consecuencias de su infracción.

Los requisitos de finalidad legítima y necesidad en una sociedad democrática apenas han tenido desarrollo jurisprudencial, por lo que deben entenderse en el sentido del segundo párrafo del artículo 8 del Convenio; es decir, que son fines legítimos "*la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*"[108].

Por último, el Tribunal hace hincapié en que la ley interna de cada Estado debe ofrecer también una serie de medidas de control para evitar los abusos, que fueron establecidas a raíz del asunto Valenzuela Contreras contra España, y confirmadas en sucesivas sentencias. A partir de estas sentencias se modificó seriamente la regulación española respecto de la interceptación de comunicaciones, fundamentalmente en el Título VIII del

[108] Art. 8.2 del Convenio para la Protección de los Derechos Humanos, op. cit. p.17.

Libro II de la Ley de Enjuiciamiento Criminal, pero también en otras leyes como la Ley General de Telecomunicaciones y la Ley Reguladora del Centro Nacional de Inteligencia.

Sin embargo, los supuestos en los que cabe esta medida están también legalmente tasados, y en ningún caso se permite la adopción prospectiva sin los suficientes indicios. En el caso de la Ley de Enjuiciamiento Criminal, se prevé para los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; en segundo lugar, delitos cometidos en el seno de un grupo u organización criminal; y en tercer lugar, los delitos de terrorismo. Sin embargo, otras leyes permiten también la adopción de estas medidas, entre las que destaca la Ley Reguladora del Centro Nacional de Inteligencia, que a diferencia de la Ley de Enjuiciamiento Criminal, se reserva su utilización en caso de que se sospechase y hubiese indicios objetivos acerca de que puede acontecer alguna situación peligrosa, amenazante o que suponga cualquier tipo de agresión contra la independencia o integridad del territorio de nuestro país, así como sus intereses o la continuidad y salvaguarda del Estado de derecho o las instituciones que lo conforman; se trata de prácticamente una copia literal de lo que el artículo 8.2 del Convenio prevé como excepciones a la regla general de que el secreto de las comunicaciones de los ciudadanos de los Estados es un derecho fundamental que debe ser respetado por las autoridades.

En definitiva, lo que en la regulación española se contempla y se trata de controlar es la interceptación de las comunicaciones personales de los particulares, impidiendo que los poderes públicos puedan realizar injerencias en las mismas salvo por los motivos legalmente establecidos y que se encuentran en consonancia con el Convenio Europeo de Derechos Humanos. Es a este tipo de comunicaciones a las que hace referencia la legislación española. No se encuentra regulado, por tanto, el ámbito de los sistemas de interceptación masivos como Echelon o Prism, sino las realizadas a individuos concretos y perfectamente identificables. Si bien es cierto que la participación de España en este tipo de programas ha sido mucho menos que testimonial, por no decir nula, el hecho de que se desconozca en el ordenamiento jurídico esta realidad no deja de ser llamativo y ciertamente preocupante. El respeto de los derechos fundamentales y más concretamente en este caso el del secreto de las comunicaciones y el de la intimidad, exigen una regulación clara respecto a las actuaciones de los poderes públicos en relación con sus ciudadanos.

6. Bibliografía

20 MINUTOS, 2013. EEUU tiene acceso a datos de los servidores de Facebook, Google, Apple, Yahoo o Skype. [en línea] 7 de junio. Disponible en: https://www.20minutos.es/noticia/1836839/0/obama-espionaje-servidores/google-facebook-skype/seguridad-nacional/ [consulta: 10 de marzo de 2020].

ALFONSO, L.P. "El derecho fundamental a la intimidad". *Ius et Praxis*, 1993, nº 21-22, pp. 39 a 56.

AUSTIN, L. "Surveillance and the Rule of Law". *Surveillance & Society*, 2015, vol. 13, nº 2, pp. 295 a 299.

Berger v. New York 388 U.S. 41 (1967).

CAMPBELL, T., et al. "El sentido del positivismo jurídico". *DOXA – Filosofía del Derecho,* 2002, vol.25, pp. 330 a 331.

CNN. 2016. ISIS dice que motivó el ataque en Berlín. [en línea] 20 de diciembre. Disponible en: https://cnnespanol.cnn.com/2016/12/20/isis-se-atribuye-responsabilidad-del-ataque-en-berlin/ [consulta: 8 de marzo de 2020]

COMUNIDAD EUROPEA. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. *DOCE* núm. 281, de 23 de noviembre de 1995, pp. 31 a 50.

Consulta sobre positivismo jurídico. En WOLTERS KLUWER: *soluciones integrales de información, software, conocimiento y formación*. [en línea]. Disponible en: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAUNTY1NjtbLUouLM_DxbIwMDC0MDI3OQQGZapUt-ckhlQaptWmJOcSoAaUZUozUAAAA=WKE [Consulta: 6-3-2020].

DÍAZ ROJO, J.A. "Privacidad: ¿neologismo o barbarismo?" *Espéculo. Revista de Estudios*, 2002.

DÍEZ RIPOLLÉS, J.L. "El bien jurídico protegido en el Derecho penal garantista". *Jueces para la democracia*, 1997, nº 30, pp. 10 a 19.

DOULIERY, O., 2013. EE. UU. tiene acceso a datos de los servidores de Facebook, Google, Apple, Yahoo o Skype. *20 Minutos*. [en línea] 7 de junio. Disponible en: https://www.20minutos.es/noticia/1836839/0/obama-espionaje-servidores/google-facebook-skype/seguridad-nacional/ [consulta: 10 de marzo de 2020]

EL ESPAÑOL, 2019. Estado Islámico reivindica el atentado del Puente de Londres: "Fue uno de nuestros combatientes". [en línea] 30 de noviembre. Disponible en: https://www.elespanol.com/mundo/20191130/islamico-reivindica-atentado-puente-londres-combatientes/448455641_0.html [consulta: 8 de marzo de 2020].

El País, *Libro de estilo: nueva versión actualizada*, 22ª ed., Madrid, 2014.

ESPAÑA. Carta de los Derechos Fundamentales de la Unión Europea. *BOE* núm. 83, de 30 de marzo de 2010, pp. 389 a 403.

ESPAÑA. Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal. *BOE* núm. 70, de 22 de marzo de 2019, pp. 30061 a 30090.

ESPAÑA. Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas. *BOE* núm. 70, de 22 de marzo de 2019, pp. 30091 a 30120.

ESPAÑA. Constitución Española. *BOE* núm. 311, de 29 de diciembre de 1978, pp. 29313 a 29424.

ESPAÑA. Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. *BOE* núm. 243, de 10 de octubre de 1979, pp. 23564 a 23570.

ESPAÑA. Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. *BOE* núm. 109, de 7 de mayo de 2002.

ESPAÑA. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. *BOE* núm. 166, de 12 de julio de 2002.

ESPAÑA. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. *BOE* núm. 114, de 10 de mayo de 2014.

ESPAÑA. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *BOE* núm. 281, de 24 de noviembre de 1995.

ESPAÑA. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. *BOE* núm. 239, de 6 de octubre de 2015, pp. 90192 a 90219.

ESPAÑA. Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. *BOE* núm. 109, de 7 de mayo de 2002, pp. 16439 a 16440.

ESPAÑA. Ley Orgánica 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal. *BOE* núm. 126, de 26 de mayo de 1988, pp. 16159 a 16160.

ESPAÑA. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. *BOE* núm. 260, de 17 de septiembre de 1882.

ESPAÑA. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. *BOE* núm. 260, de 17 de septiembre de 1882.

ESTEVE ROMERO, A. *Arqueología informática: Implementación de sistemas clásicos de cifrado en Scratch*. MOLERO PRIETO, Xabier (dir.). Tesis Doctoral. Universitat Politècnica de València. Departamento de Informática de Sistemas y Computadores, 2019.

EUROPOL. Changes in modus operandi of Islamic State (IS) revisited'. *The Hague*, 2016.

FAJARDO URIBE, L.A. "A propósito de la comunicación verbal". *Forma y función*, 2009, volumen 22, nº2, pp. 121 a 142.

FERRER MORINI, T., 2013. Diccionario del espionaje digital. *El País*. [en línea]. 26 de octubre. Disponible en: https://elpais.com/internacional/2013/10/26/actualidad/1382810941_379301.html [consulta: 10 de marzo de 2020]

GELMANN, B., 2013. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. [en línea]. Disponible en: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [consulta: 10 de marzo de 2020]

GONZÁLEZ MONJE, A. "Amenazas a la seguridad y privacidad: la dificultad del equilibrio perfecto". *Revista europea de derechos fundamentales*, 2017, nº 29, pp. 267 a 294.

GONZÁLEZ PORRAS, A.J. *Privacidad en internet: los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva*. PÉREZ PEDRERO, Enrique Belda (dir.). Tesis doctoral, Universidad de Castilla-La Mancha, Departamento de Derecho Constitucional. 2016.

GREENWALD, G. 2013. NSA collecting pone records of millions of Verizon customers daily. *The Guardian*. [en línea] 6 de junio. Disponible en: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [consulta: 8 de marzo]

GUTIÉRREZ ZARZA, M.A. "Terrorismo yihadista, crisis migratorias, fronteras, prueba electrónica, encriptado, referéndum y otras palabras clave del espacio LSJ en 2016". *Diario La Ley*, 2017, nº 8904, p. 3.

JIMENO-BULNES, M. "The use of intelligence information in criminal procedure: A challenge to defence rights in the European and the Spanish panorama". *New Journal of European Criminal Law*, 2017, vol. 8, nº 2, pp. 171 a 191.

JOSKOWICZ, J. "Breve historia de las telecomunicaciones". *Instituto de Ingenieria Eléctrica de la republica de Uruguay,* 2013.

Katz v. United States 389 U.S. 347, 351 (1967).

LA RAZÓN, 2019. La barbarie yihadista relatada desde dentro del Charlie Hebdo. [en línea] 29 de agosto. Disponible en: https://www.larazon.es/cultura/la-barbarie-yihadista-relatada-desde-dentro-del-charlie-hebdo-LD24729165/ [consulta: 8 de marzo de 2020]

MALDONADO, C.E. "La red Echelon: el control de internet y de todas las comunicaciones". *Le Monde diplomatique*, 2013, pp. 30 a 31

Mapp v. Ohio, 367 U.S. 643 (1961).

MARTÍN LÓPEZ, S. *Programas de vigilancia de Internet*. PÉREZ SOLÀ, Cristina (dir.). Trabajo de fin de máster, Universitat Oberta de Catalunya, Máster Interuniversitario en seguridad de las tecnologías de la información y de las comunicaciones (MISTIC), 2014.

NIEVES SALDAÑA, M. "El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego". *Teoría y Realidad Constitucional*, 2011, nº28, pp. 279 a 312.

NIEVES SALDAÑA, M. "La protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de la información personal en los Estados Unidos". *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades*, 2007, vol. 9, nº 18, pp. 85 a 115.

Olmstead v. United States, 277 U.S. 438 (1928)

PARLAMENTO EUROPEO. 2013. Documento de Trabajo 1 sobre los programas de vigilancia de los Estados Unidos y la UE, y su repercusión sobre los derechos fundamentales de los ciudadanos europeos.

PARLAMENTO EUROPEO. 2013. Programa de vigilancia de la ANS de los EE.UU., servicios de inteligencia en varios Estados miembros e impacto en la privacidad de los ciudadanos de la UE.

PARLAMENTO EUROPEO. Informe sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación ECHELON) (2001/2098 (INI)). 2001.

PIODI, F.; MOMBELLI, I. The ECHELON Affair: The EP and the global interception system 1998–2002. 2014.

QUINTANA, Y., 2014. Todos los programas de espionaje de la NSA desvelados por Snowden. *Eldiario*. [en línea]. 19 de marzo. Disponible en: https://www.eldiario.es/turing/vigilancia_y_privacidad/NSA-programas-vigilancia-desvelados-Snowden_0_240426730.html [consulta: 10 de marzo de 2020]

REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.3 en línea]. https://dle.rae.es/privacidad?m=form [1 de marzo de 2020].

REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.3 en línea]. https://dle.rae.es/privado [1 de marzo de 2020].

REAL ACADEMIA ESPAÑOLA: *Diccionario de la lengua española*, 23.ª ed., [versión 23.3 en línea]. https://dle.rae.es/intimidad?m=form [1 de marzo de 2020]

RIVERA, N., 2016. Cronología del caso Snowden, el hombre más buscado el mundo. *Hipertextual*. [en línea] 15 de marzo. Disponible en: https://hipertextual.com/2016/03/cronologia-edward-snowden [consulta: 10 de marzo de 2020]

RODRÍGUEZ RUBIO, C. "La injerencia en el derecho al secreto de las comunicaciones a través de la regulación de las medidas de investigación tecnológica". *Revista europea de derechos fundamentales*, 2016, nº 28, pp. 267 a 285.

RUIZ MIGUEL, C., *La configuración constitucional del derecho a la intimidad*. LUCAS VERDU, P. (dir.). Tesis doctoral, Universidad Complutense de Madrid, Departamento de Derecho Constitucional, 1995.

SALAMANCA AGUADO, E. "El respeto a la vida privada ya la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones". *Revista del Instituto Español de Estudios Estratégicos*, 2014, nº 4.

SANTOS, F.R. "El Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos de América y la propuesta de lege ferenda en el derecho comunitario". *Diario La Ley*, 2017, nº 9004, p. 2.

SERRA CRISTÓBAL, R. “La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional”. *Revista de Derecho Político*, 2015, vol. 92, pp. 73 a 118.

SERRA CRISTÓBAL, R. “Los derechos fundamentales en la encrucijada de la lucha contra el terrorismo yihadista. Lo que el constitucionalismo y el derecho de la Unión Europea pueden ofrecer en común”. *Teoría y realidad constitucional*, 2016, vol. 38, pp. 487 a 503.

STC nº 175/2000, de 26 de junio.

STEDH 13 de junio de 1979, as. C-6833/74 *Marckx vs. Belgium*

STEDH 18 de diciembre de 1986, as. C-9697/82, *Johnston and others vs. Ireland*

STEDH 18 de febrero de 2003; as. C-58496/00 *Prado Bugallo vs. Spain*.

STEDH 2 de agosto de 1984, as. C-8691/79 *Malone vs. The United Kingdom*

STEDH 22 de octubre de 1981, as. C-7525/76, *Dudgeon vs. The United Kingdom*

STEDH 24 de abril de 1990, as. C-11801/85, *Kruslin vs. France*

STEDH 25 de marzo de 1983, as. 5947/72 *Silver and others vs. The United Kingdom*

STEDH 26 de abril de 1979, as. C-6538/74 *The Sunday Times vs. The United Kingdom*

STEDH 26 de marzo de 1985, as. C-8978/80 *X and Y vs. The Netherlands*

STEDH 29 de junio de 2006, as. C-54934/00 *Weber and Sarabia vs. Germany*

STEDH 3 de abril de 2007, as. C-62617/00, *Copland vs. The United Kingdom*

STEDH 30 de julio de 1998, as. C-27671/95 *Valenzuela Contreras vs. Spain*

STEDH 6 de septiembre de 1978, as. C-5029/71, *Klass and others vs. Germany*

STS de 16 de mayo de 2014.

STS de 17 de diciembre de 2009

STS de 20 de septiembre de 2005

STS de 22 de diciembre de 2011.

STS de 22 de julio de 2013.

STS de 24 de marzo de 2003.

STS de 28 de septiembre de 2015.

STS de 9 de marzo de 2007.

TELEMADRID, 2019. Se cumplen 18 años del atentado terrorista del 11-S. [en línea]. 11 de septiembre de 2019. Disponible en: http://www.telemadrid.es/programas/telenoticias-1/anos-atentado-terrorista-11-S-2-2157704242--20190911043523.html [consulta: 8 de marzo de 2020]

UNIÓN EUROPEA. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). DOUE núm. 201, de 31 de julio de 2002, pp. 37 a 47.

VANDERLINDER, I. "Los derechos humanos ante la vigilancia indiscriminada de las comunicaciones privadas". *Revista UVM*. 2016, volumen 10, nº2.

VILLEGAS GARCÍA, M.A. "La sentencia Carpenter v. United States:¿ La primera gran victoria de la privacidad en la era digital?". *Diario La Ley*, 2018, nº 9316, p. 2.

YÁRMOS, C. 2016. El ISIS se responsabiliza de la matanza de Niza. *El País*. [en línea] 16 de julio. Disponible en: https://elpais.com/internacional/2016/07/16/actualidad/1468654029_015759.html [consulta: 8 de marzo de 2020]